DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO/IEC 27001 PARA LA EMPRESA USOMET LTDA. EN LA CIUDAD DE IBAGUÉ

JAIME HERNANDO HENAO RODRÍGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2016

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO/IEC 27001 PARA LA EMPRESA USOMET LTDA. EN LA CIUDAD DE IBAGUÉ

JAIME HERNANDO HENAO RODRÍGUEZ

Proyecto de grado requisito para optar el título de ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Asesor: SALOMÓN GONZÁLEZ GARCÍA.
Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2016

NOTA DE ACEPTACIÓN

_____
_____
_____
_____

_____

Firma del Jurado 1

_____

Firma del Jurado 2

Bogotá Día: ____ Mes____ Año: 2016

AGRADECIMIENTO

Reconozco que el apoyo de los docentes de la UNAD ha sido de gran valor para elaborar en forma adecuada desde el anteproyecto hasta el proyecto de grado, por su paciencia, aportes, sugerencias, comentarios y revisiones muchas gracias.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE IMÁGENES

Pág.

RESUMEN

El presente proyecto tiene como finalidad crear el diseño del sistema de gestión de seguridad de la información para la empresa USOMET de la ciudad de Ibagué, con el fin de mitigar las amenazas, vulnerabilidades y riesgos presentes en cada uno de sus activos.

Palabras Claves:

ISO/IEC 27001:2013, SGSI, Vulnerabilidad, Riesgo, Amenaza, Activos de Información, MAGERIT, Gestión de Riesgo, Control, Políticas de seguridad.

INTRODUCCIÓN

Aún hoy día ya conocidos los riesgos de seguridad a los que están expuestos los activos de las tecnologías de la información y comunicaciones (TICs), se encuentran entidades, empresas y organizaciones en las que no se cuenta con un sistema de gestión en seguridad de la información para preservar la disponibilidad, integridad y confidencialidad de sus activos informáticos. Este proyecto de diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001:2013 y siguiendo la metodología MAGERIT para la empresa USOMET Ltda. en la ciudad de Ibagué, se realiza en el 2016 para determinar cuáles son sus activos informáticos y a qué amenazas, vulnerabilidades y riesgos están expuestos y en qué grado, para finalmente determinar los controles que permitan incrementar la seguridad al interior de la organización.

1. TÍTULO DEL PROYECTO

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO/IEC 27001 PARA LA EMPRESA USOMET LTDA. DE LA CIUDAD DE IBAGUÉ

2. PLANTEAMIENTO DEL PROBLEMA

2.1 DESCRIPCIÓN DEL PROBLEMA

USOMET Ltda es una empresa dedicada a prestar los servicios de salud y está ubicada en la ciudad de Ibagué. Inició sus actividades en marzo de 1990 y respondiendo a los lineamientos establecidos por la Resolución 01016 de 1989, atendiendo las necesidades en materia de salud ocupacional de las diferentes empresas que se encontraban en la necesidad de esta clase de servicios.

Actualmente, USOMET Ltda. está dedicada a la gestión en salud ocupacional para empresas de todos los sectores económicos del departamento del Tolima. Parte de su labor es la de llevar el registro de la información de las ARL contratantes, las empresas que las ARL le asignan, los empleados vinculados o a ser vinculados por esas empresas, los resultados de los estudios y capacitación en salud ocupacional que en ellas se gestionan, los resultados de las evaluaciones médicas y de laboratorio de los empleados.

Es por ello, que la empresa maneja un importante volumen de información en la gestión de la operación normal de la misma. A pesar de la gran cantidad de información que se maneja en la organización no se cumple con las premisas básicas de la seguridad de la información: la confidencialidad, integridad y disponibilidad.

El presente proyecto busca mitigar las diversas vulnerabilidades que afectan al sistema informático de USOMET a través del diseño de un Sistema de gestión que permita mitigar los riesgos y resguardar la información que se almacena.

2.2 FORMULACIÓN DEL PROBLEMA

¿Cómo el diseño del SGSI basado en la norma ISO/IEC 27001:2013 contribuirá a mejorar la seguridad aumentando la competitividad de la empresa USOMET LTDA.?

3. JUSTIFICACIÓN DEL PROYECTO

USOMET Ltda. sufrió la materialización de amenazas que han preponderado su activo más importante: la información, por lo que es prioritario el salvaguardar sus activos informáticos estableciendo los elementos de seguridad necesarios de acuerdo a lo establecido por la norma ISO/IEC 27001:2013 y mediante la metodología MAGERIT.

La investigación se centra en el estudio de seguridad sobre los activos informáticos de la empresa por tanto requieren ser identificados, inventariados y evaluados de acuerdo a sus amenazas, vulnerabilidades y riesgos.

Al verse vulnerada la información por diversas situaciones de tipo laboral, organizacional o de cualquier índole es necesario mejorar las condiciones actuales y establecer una serie de protocolos de acuerdo a lo que estípula la norma ISO/IEC 27001:2013.

Por lo tanto, para evitar que sea menoscabada la confianza del personal de la empresa, los clientes y los usuarios en el sistema de información, se hace necesario el levantamiento de inventario de activos, sus vulnerabilidades, amenazas, riesgos y grado de exposición, para determinar así los controles que deberán aplicarse poniendo en marcha la implementación de un sistema de gestión de seguridad de la información.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Facilitar la administración de la seguridad informática y de la información mediante el diseño de un manual de políticas y procedimiento que apoyen el SGSI basado en la norma ISO/IEC 27001:2013 aumentando la competitividad de la empresa USOMET LTDA.

4.2 OBJETIVOS ESPECÍFICOS

Diagnosticar las condiciones actuales de la empresa USOMET Ltda., en lo relacionado en materia de información y seguridad informática, identificando sus activos informáticos, mediante instrumentos de recolección de información.

Caracterizar los procesos de manejo de información en USOMET con el fin de evaluar e identificar las vulnerabilidades, amenazas y riesgos, relacionados con los activos informáticos.

Definir mecanismos de gestión de seguridad informática basados en la norma ISO/IEC 27001:2013 que faciliten la solución de problemas mediante la aplicación de políticas y procedimientos.

Diseñar el manual de políticas para el sistema de gestión de seguridad de la información.

5. MARCO DE REFERENCIA

5.1 MARCO TEÓRICO

Dentro de los estándares desarrollados para gestionar la seguridad de la información se encuentra la norma ISO/IEC 27001:2013, aplicada en el desarrollo de este proyecto. Específicamente se siguen las normas ISO/IEC 27001:2013 e ISO/IEC 27002, así como la metodología MAGERIT para la determinación del riesgo y su control, mediante la valoración de las vulnerabilidades, amenazas y riesgos sobre los activos informáticos. Para su determinación se tendrá en cuenta el factor cultural que tiene una gran incidencia en el buen o mal manejo que se dé a la seguridad de la información en cualquier entorno donde se cuente con una infraestructura informática.

Como parte de la norma ISO/IEC 27001:2013 se establecen las especificaciones para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un sistema de gestión de seguridad de la información (SGSI), manejando un enfoque por la aplicación de controles de forma que la gestión de la seguridad de la información se realiza como un proceso sistemático y documentado, que debe ser conocido por todo el personal vinculado a la organización o empresa.

Como parte de las especificaciones de la norma se debe establecer un sistema de documentación para el SGSI que debe ser actualizado y divulgado periódicamente entre los usuarios del sistema. Esta documentación debe contener la política de seguridad aprobada para la empresa.

Las políticas y los procedimientos son reglas que deben cumplirse para poder garantizar una óptima protección de los activos informáticos, pues son desarrolladas técnicamente bajo la observación de normas internacionales de amplio reconocimiento y aceptación.

5.1.1 Seguridad de la Información. La seguridad de la información, según ISO/IEC 27001:2013, es la aplicación de mecanismos que garanticen la confidencialidad, integridad y disponibilidad de todos los activos informáticos involucrados.

Significa poner en práctica: políticas, procedimientos y protocolos; determinados por una serie de normas en las que se establecen las medidas necesarias de protección.

Las empresas que adoptan la seguridad de la información aseguran que su sistema no sea vulnerado bajo ninguna circunstancia previsible y minimizan al máximo los posibles daños que puedan ocurrir si se llega materializar una contingencia.

5.1.2 Análisis de Riesgos Informáticos. El análisis de riesgos no cuenta con una única definición pues se han redactado muchas definiciones dependiendo de las situaciones analizadas. Para algunos es una situación que se presenta en un lugar y momento específico, pero con consecuencias que pueden llegar a afectar el normal desempeño de todo o parte del sistema. Para otros, el riesgo es inherente a los sistemas en sí mismos, pues son parte del mundo real en que por diversas circunstancias los riesgos se materializan, generando afectación en mayor o menor grado a los activos informáticos.

En este orden de ideas, el Análisis de Riesgos es la actividad más importante dentro de la gestión de la seguridad de la información en una empresa u organización, pues de allí se deriva el establecimiento de las medidas de manejo del riesgo y las decisiones que conforman las políticas de seguridad.

5.1.3 Metodología de Análisis de Riesgos. Se desarrolla a partir de la identificación de los activos informáticos y la ausencia de controles sobre los mismos, analizando:

- Activos
- Amenazas
- Vulnerabilidad
- Riesgos
- Salvaguardas

En un sistema de Gestión de la Seguridad de la Información (SGSI) definido por la norma ISO/IEC 27001:2013, se deben tener en cuenta características culturales de la empresa, debe ser ajustado periódicamente conforme la capacidad de la empresa u organización para introducir mejoras en forma permanente.

Para desarrollar y establecer un Sistema de Gestión de la Seguridad de la Información con base a ISO/IEC 27001:2013, se debe definir el alcance del SGSI en términos de la organización, su localización, activo y tecnología. Una vez identificados estos componentes se procede a calcular el riesgo que afecta a los activos y se diseña la política de seguridad con:

- Objetivos y marco general de seguridad de la información de la empresa.
- Requerimientos legales o contractuales relativos a la seguridad de la información.
- Contexto estratégico de gestión de riesgos de la empresa.

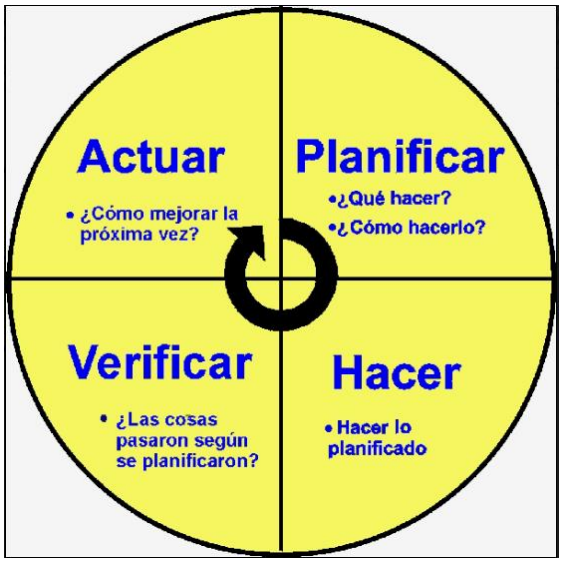
Con base a esto se propone establecer el mejoramiento en los procesos de seguridad de la información y su aplicabilidad en los procesos identificados.

5.1.4 MAGERIT. (Metodología de análisis y Gestión de Riesgos de los Sistemas de Información), desarrollada por CSAE (Consejo Superior de Administración Electrónica) metodología desarrollada como respuesta a la necesidad de hacer frente al creciente uso de medios electrónicos para el manejo de la información en todas sus formas: generación, procesamiento, comunicación, registro, respaldo. De esta manera en la norma se reúne un conjunto de las mejores prácticas para brindar seguridad en el manejo de la información.

5.1.5 CICLO DE DEMING. La norma ISO/IEC 27001:2013 realiza el análisis de procesos con apoyo en el ciclo Deming. Este análisis plantea la gestión de la seguridad como un proceso de mejora continua, imagen 1, aplicando la repetición cíclica de cuatro fases:

- **Planificar**: Realizar la planeación significa establecer los objetivos y definir los medios que permitirán su logro.
- **Hacer**: Llevar a cabo las acciones planeadas para el logro de los objetivos empleando los medios preestablecidos.
- **Verificar**: Seguimiento que trata de establecer el grado de avance en la consecución de los objetivos planeados.
- **Actuar**: Luego de realizar el análisis de la verificación, se debe estudiar y definir y aplicar los correctivos que sean necesarios encaminar nuevamente la acción hacia el logro de los objetivos.

Imagen 1 Ciclo DEMING



Fuente: http://gestionxprocesoscun.blogspot.com.co/2015/04/el-ciclo-de-deming.html

5.2 MARCO CONCEPTUAL

Amenaza: Todo aquello que pueda llegar a afectar de alguna forma la seguridad de la información del sistema informático. Una amenaza es la posibilidad de aprovechamiento de las vulnerabilidades.

Confidencialidad: Dentro de una plataforma informática. Servicio que ofrece la capacidad para controlar que a determinada información solo tenga acceso las personas procesos autorizados y entidades autorizadas.

Disponibilidad: El acceso a datos de un sistema de información debe estar garantizado siempre que sea requerido, por lo cual no debe haber inconveniente de ningún orden para que la quienes deban usarla la tengan a su alcance.

Integridad: La información que se administre en un sistema de informático debe conservarse libre de alteraciones no autorizadas. La violación de la integridad puede concretarse cuando hay modificación de los datos ya sea por una persona, un programa o un dispositivo electrónico; alterando los contenidos, modificándolos o borrándolos en su totalidad o parcialmente, sin que sea un procedimiento autorizado.

Riesgo: Se identificarán como cualquier impedimento, obstáculo, amenaza o problema que al afectar el sistema de información pueda impedir que los usuarios autorizados alcancen sus objetivos. Es también la posibilidad de sufrir un daño o pérdida, medible en términos de impacto y de probabilidad de ocurrencia.[1].

Vulnerabilidades. Identificadas como aquellas debilidades existentes en el sistema de información y que comprometen la seguridad de los datos, pudiendo llegar a su perdida. Es un elemento de riesgo interno, que representa la factibilidad con que los activos o el sistema completo sean afectados por el fenómeno que caracteriza la amenaza.

5.3 MARCO HISTÓRICO

La ISO, International Organization for Standardization, 'Organización Internacional de Estandarización'. Órgano responsable del sistema de normalización internacional para productos de diversas áreas.

Entre sus normas la ISO/IEC 27001:2013 establece requisitos para implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. Este estándar se publicó por la ISO y por la comisión International Electrotechnical Commission en octubre del año 2005. Actualmente es el único estándar aceptado a nivel internacional para la gestión de la Seguridad de la Información. La evolución de la norma ISO/IEC 27001:2013 se deriva de estándares anteriores relacionados con la seguridad de la información y que se relacionan a continuación:

- 1901 – Normas “BS”: La British Standards Institution publica normas con el prefijo “BS” con carácter internacional, donde se originan las normas: ISO 9001, ISO 14001 u OHSAS 18001.

- 1995- BS 7799-1:1995: Mejores prácticas para ayudar a las empresas británicas a administrar la Seguridad de la Información. Normas que no contemplaban certificación.

- 1998 – BS 7799-2:1999: Revisión de la anterior norma. Establecía los requisitos para implantar un Sistema de Gestión de Seguridad de la Información certificable.

- 1999 – BS 7799-1:1999: Se revisa toda la norma corrigiendo errores.

[1] INTERNATIONAL STANDARD ISO/IEC 17799:2005 ,Iso-Iec 17799 2005.pdf, 2005

- 2000 – ISO/IEC 17799:2000: La Organización Internacional para la Estandarización (ISO) tomó la norma británica BS 7799-1 que dio lugar a la llamada ISO 17799, sin experimentar grandes cambios.

- 2002 – BS 7799-2:2002: Se publicó una nueva versión que permitió la acreditación de empresas por una entidad certificadora en Reino Unido y en otros países.

- 2005 – ISO/IEC 27001:2005 e ISO/IEC17799:2005: Aparece el estándar ISO 27001 como norma internacional certificable y se revisa la ISO 17799 dando lugar a la ISO 27001:2005.

- 2007 – ISO 17799: Se renombra y pasa a ser la ISO 27002:2005

- 2007 – ISO/IEC 27001:2007: Se publica la nueva versión.

- 2009 – Se publica un documento adicional de modificaciones llamado ISO 27001:2007/1M:2009.

En el año 2013 fue publicada la nueva versión de la ISO 27001 que trae cambios significativos en su estructura, evaluación y tratamiento de los riesgos.

5.4 MARCO LEGAL

Para el desarrollo del proyecto se tienen en cuenta las siguientes normas:

Código procesal penal de 1987, que tutela la inviolabilidad del domicilio y regula en su artículo 376 las escuchas telefónicas.

Ley de Protección de datos de 1988.

Ley 72/1989, de 20 de diciembre de 1989, por la cual se definen nuevos conceptos y principios sobre la Organización de las Telecomunicaciones en Colombia y sobre el régimen de concesión de los servicios y se confieren unas facultades extraordinarias al Presidente de la República.

Decreto 1794/1991, de 16 de julio de 1991, por el cual se Expiden Normas sobre los Servicios de Valor Agregado y Telemáticos y se Reglamenta el Decreto 1900 de 1990.

Decreto 2150 de 1995 sobre sistemas electrónicos, de 5 de diciembre de 1995, que busca la simplificación de trámites ante Entidades Estatales. (Diario Oficial 42.137, del 6 de diciembre de 1995).

Resolución 087 de 5 de septiembre de 1997, de la Comisión de Regulación de las Telecomunicaciones, por medio de la cual se regula en forma integral los servicios de Telefonía Pública Básica Conmutada (TPBC) en Colombia.

Proyecto de Ley 227 de 21 de abril de 1998, por medio del cual se define y Reglamenta el Acceso y el uso del Comercio Electrónico.

Ley 527 de 18 de agosto de 1999, sobre Mensajes de Datos, Comercio electrónico y Firma Digital.

Resolución 7652/2000, de 22 de septiembre de la Dirección General de Impuestos y Aduanas Nacionales, por la cual se reglamenta la administración, publicación y uso de la información electrónica vía INTRANET e INTERNET en la Dirección de Impuestos y Aduanas Nacionales.

Proyecto de Ley 166 de 31 de enero de 2003, por el cual se regulan las comunicaciones Vía Internet y mediante el uso de Fax que se realicen desde lugares habilitados para brindar al público esos servicios.

Proyecto de Ley 05/2006 Senado "Por el cual se reglamenta el Habeas Data y el Derecho de Petición ante Entidades Financieras, Bancarias y Centrales o Banco de Datos". Acumulado Proyecto de Ley nº 27/2006 Senado "Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera y crediticia, y se dictan otras disposiciones". Aprobado por la comisión el día 12 de octubre de 2006.

Informe de Conciliación al Proyecto de Ley Estatutaria 221/2007 de 4 de junio de 2007, sobre el Derecho de Habeas Data.

Decreto 2870 de 31 de julio de 2007, por medio del cual se adoptan medidas para facilitar la Convergencia de los servicios y redes en materia de Telecomunicaciones. (Diario oficial nº 46.706 de 31 de julio de 2007).

Resolución 1732 de 17 de septiembre de 2007, de la Comisión de Regulación de Telecomunicaciones, con el que se expide el Régimen de Protección de los Derechos de los Suscriptores y Usuarios de los Servicios de Telecomunicaciones. (Diario Oficial nº 46.756 de 19 de septiembre de 2007)

Ley 1266 de 31 de diciembre de 2008, por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de información administrada en

bases con datos personales, en especial: la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. (Diario Oficial nº 47.219).

Ley 1273 de 5 de enero de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones (Diario Oficial nº 47.223).

Ley 1341 de 30 de julio de 2009, sobre principios y conceptos referentes a la Sociedad de la Información y la organización de las Tecnologías de la Información y las Comunicaciones (Diario Oficial nº 47426 de 30 de julio de 2009).

Decreto 2888 de 4 de agosto de 2009, del Ministerio de Tecnologías de la Información y las Comunicaciones, por el cual se dictan disposiciones sobre la organización y funcionamiento de la Comisión de Regulación de Comunicaciones – CRC.

Resolución 2251 del 11 de diciembre de 2009, de la Comisión de Regulación de las Comunicaciones, por la cual se modifica la Resolución 1914 de 2008 de la CRT.

Resolución 2554 de 19 de mayo de 2010, de la Comisión de Regulación de las Comunicaciones, Modificación al Régimen de Protección de los Derechos de los Usuarios de Servicios de Telecomunicaciones.

Comisión de Regulación de Comunicaciones de 30 de junio de 2010, Acceso a Redes por parte de proveedores de contenidos y aplicaciones.

5.6 MARCO CONTEXTUAL

La empresa USOMET Ltda., inició sus actividades en marzo de 1990, con tres socios fundadores, las instalaciones se ubicaron en la carrera 5ª con calle 40, inicialmente, se vinculó un médico y un ingeniero industrial, quienes posteriormente hicieron la especialización en salud ocupacional.

Respondiendo a los lineamientos estipulados por la Resolución 01016 de 1989, la empresa USOMET atiende las solicitudes en relacionadas con la salud ocupacional de las diferentes empresas que reconocen la necesidad de este servicio.

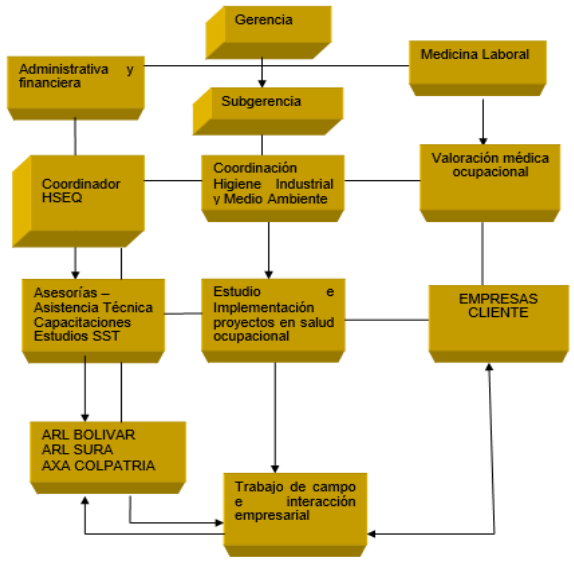
Luego del primer año, USOMET atendía dos empresas, en actividades centradas en la seguridad industrial y medicina del trabajo, con énfasis en estadísticas de accidentalidad y práctica de exámenes paraclínicos de: audiometría, visiometría y espirometría.

Hacia el año 1994, USOMET bajo la licencia inicialmente a 5 años, renovada a 10 años, prestó sus servicios a 25 empresas, cuyas actividades se realizaron de conforme cronogramas de actividades estipulados en documentos que se diseñaron para las empresas afiliadas.

En 1993 nace la Ley 100/93 y con ella la necesidad del Decreto 1295/94 reglamentario de esta Ley que amplía la información y apoyo hacia la salud ocupacional de las empresas, aparecen las administradoras de riesgos profesionales (A.R.L.s privadas), quienes posteriormente van a dar el apoyo y acompañamiento para la ejecución de actividades a las empresas de diferentes sectores a partir de esta nueva legislación.

USOMET, cuenta con una planta de personal de ocho personas (médico especialista en salud ocupacional, ingeniero industrial especialista en salud ocupacional y otros profesionales en salud ocupacional, todos con licencia expedida por la Secretaría de Salud, igualmente tiene personal directivo en gerencia y subgerencia, personal operativo: secretaría, administrativa y financiera, coordinación en seguridad y logística, Higiene Industrial y Medio Ambiente). El organigrama de la empresa se puede visualizar en la siguiente ilustración:

Imagen 2 Organigrama USOMET Ltda.



Fuente: USOMET Ltda

5.7 MARCO DE ANTECEDENTES

Para aproximar esta investigación sobre cómo mejorar la seguridad de los activos informáticos de una empresa mediante los lineamientos de un SGSI, se realizó la consulta de anteriores trabajos de grado relacionados con el tema a fin de conocer los avances logrados en ese sentido. Entre los más importantes se pueden mencionar:

- El trabajo de grado presentado en abril de 2015 en la Universidad Nacional Abierta a Distancia (UNAD), titulado: “Diseño de un sistema de gestión de la seguridad informática SGSI, para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C. a través de la auditoría.”, como requisito para optar al título de Especialista en Seguridad informática por parte del Ing. Alexander Guzmán García[2].

Esta investigación trata sobre el diseño de un SGSI para mejorar la seguridad informática en empresas del sector textil en tres ciudades de Colombia. Recolectando información de los riesgos, diseñando los medios para la recolección de información, aplicando los instrumentos que permiten evidenciar las vulnerabilidades y amenazas; para finalmente diseñar e implementar un SGSI.

- El trabajo de grado presentado en 2015 en la Universidad Nacional Abierta a Distancia (UNAD), titulado: “*Estudio de los Procesos de Seguridad de la Información Digital en las Empresas del Departamento de Risaralda.*”, como requisito para optar al título de Especialista en Seguridad informática por parte del ingeniero: Oscar Andrés Sierra Jaramillo[3].

Esta investigación detalla acerca el estudio de la aplicación de las normas 27001 de seguridad de la información en empresas de Risaralda, realizando encuestas para verificar la aplicación de las políticas de las normas ISO/IEC 27001:2013 y la ISO 27002, realizando el análisis de los resultados estableciendo los niveles de seguridad en uso, para finalmente proponer los modelos de seguridad aplicables a las empresas evaluadas.

[2] A. G. García, "Diseño de un sistema de gestión de la seguridad informática SGSI, para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C. a través de la auditoría". [En línea]. Available: repository.unad.edu.co/bitstream/10596/3448/1/1030548291.pdf.

[3] O. A. S. Jaramillo, "Estudio de los procesos de seguridad de la información," 2008. [En línea]. Available: http://repositorio.utp.edu.co/dspace/bitstream/11059/2370/1/0058S572.pdf.

6. METODOLOGÍA

6.1 TIPO DE INVESTIGACIÓN

El paradigma de investigación es de tipo cuantitativo, ya que supone la medición de vulnerabilidades, amenazas y riesgos de seguridad de acuerdo a escalas de medición indicados en la metodología MAGERIT para el análisis de riesgos.

Este tipo de investigación es descriptiva porque describe los procesos, servicios, activos informáticos, las vulnerabilidades, amenazas y riesgos existentes en USOMET.

6.2 LÍNEA DE INVESTIGACIÓN

Se aplica la línea de investigación: gestión de sistemas que hace referencia a la indagación en sus dinamismos por medio de la evolución de las tecnologías de la información.

6.3 METODOLOGÍA DE DESARROLLO

Para el logro de los objetivos propuestos se desarrollarán las siguientes actividades conforme cada objetivo.

Objetivo 1: Diagnosticar y evaluar las condiciones actuales de la empresa USOMET Ltda., en lo relacionado en materia de información y seguridad informática, identificando sus activos informáticos, mediante instrumentos de recolección de información.

Actividades:

- Realizar visitas a la empresa para identificar los activos informáticos existentes, registrando cada uno en los formatos prediseñados.
- Solicitar información sobre los inventarios de los activos informáticos.
- Entrevistar a los responsables del área informática para determinar los activos informáticos que soportan el sistema de información.

Objetivo 2: Caracterizar los procesos y procedimientos de manejo de información en USOMET con el fin de evaluar e identificar las vulnerabilidades, amenazas y riesgos, relacionados con los activos informáticos.

Actividades:

- Solicitar información sobre los funcionarios y procesos que cada uno realiza sobre los activos informáticos.

- Acompañar en su labor a los funcionarios que realizan actividades que involucran los activos informáticos.

- Registrar los hallazgos de vulnerabilidades, amenazas y riesgos, sobre su forma de uso en instrumentos de medición previamente diseñados.

Objetivo 3: Definir mecanismos de gestión de seguridad informático basados en la norma ISO/IEC 27001:2013 que faciliten la solución de problemas mediante la aplicación de políticas y procedimientos.

Actividades:

- Definir políticas de seguridad de la información para el manejo de los activos de la empresa.

- Establecer procedimientos de manejo apropiado para los diferentes tipos de activos identificados.

- Validar con la gerencia de USOMET las políticas y procedimientos generados.

Objetivo 4: Diseñar la política de seguridad y controles para el sistema de gestión de seguridad de la información.

Actividades:

- Indicar controles a aplicar conforme el estudio realizado.

- Elaborar la política de seguridad.

6.4 POBLACIÓN Y MUESTRA

La población objeto de este proyecto es el personal de la empresa USOMET ubicada en la ciudad de Ibagué. Como muestra se trabajará sobre el 100% del personal vinculado a la empresa pues es bastante pequeña.

6.5 ALCANCE Y DELIMITACIÓN DEL PROYECTO

Elaborar un manual de políticas y procedimientos teniendo en cuenta el estudio realizado en la empresa y de acuerdo a los riesgos encontrados en la organización.

El proyecto se aplicará puntualmente sobre el área informática de la empresa USOMET Ltda con ubicación en la ciudad de Ibagué, Tolima. La gestión se llevará a cabo durante el segundo semestre de 2016, con una duración de 13 semanas.

7. ACTIVOS DE INFORMACIÓN

Un activo es toda información que se gestione en un sistema informático en conjunto con los dispositivos y software con que se administran por parte de cualquier persona o entidad y que deban ser protegidos frente a posibles riesgos y amenazas por ser fundamental para el logro de los objetivos de la empresa u organización.

7.1 IDENTIFICACIÓN DE ACTIVOS

En la tabla 1 se elabora una relación de los activos informáticos identificados en la empresa.

Tabla 1 Activos informáticos USOMET Ltda.

TIPO DE ACTIVOS	NOMBRE	CARACTERÍSTICAS
COMUNICACIONES [COM]	Router	Dlink – 524 Tecnología 802.11g/2.4 GHz. Wireless Router.
	Modem	Arris TG862
HARDWARE [HD]	Impresoras Escáner	Cuatro impresoras HP Deskjet F4480. Impresora, escáner y copiadora.
	UPS	UPS centralizada marca Delta de capacidad 10 KW.
	Computadores	Portátiles 4 Pc's de escritorio 4 Servidor 1
	Servidor	HP Proliant
SOPORTE DE INFORMACIÓN FÍSICA	Documentos	Para toda la documentación se cuenta con dos archivadores verticales con separadores para carpetas organizados por año, mes, contenido. Para toda la documentación de la empresa

INFORMACIÓN DIGITAL [ID]	Archivos de información.	La empresa cuenta con soportes para los archivos de información manejados por los ordenadores como son: los discos magnéticos o discos duros, los discos ópticos (CD, DVD), tarjetas de memoria USB.
PERSONAL [P]	Empleados	Actualmente cuenta con 10 empleados que hacen uso del sistema de información.
SOFTWARE [SF]	Sistema operativo	Todos los equipos están actualizados a Windows 10
	Software antivirus	Windows Defender en todos los equipos
	Firewall	De Windows activo en todos los equipos
	Bases de datos	Ninguna
	Ofimática	Office 2013
	Correo Electrónico	Basado en Gmail

Fuente: el autor

7.2 VALORACIÓN DE ACTIVOS

Para la valoración de activos se ha establecido el análisis de las dimensiones indicadas en la tabla 2:

Tabla 2 Dimensiones de Seguridad para la Identificación y Valoración de Amenazas en MAGERIT.

DIMENSIÓN DE SEGURIDAD	NOMENCLATURA	DEFINICIÓN
Disponibilidad	D	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008].
Integridad	I	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004].
Confidencialidad	C	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007].

Autenticidad	A	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008].
Trazabilidad	T	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008].

Fuente: AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 15-16.

En la tabla 3 se indican los niveles de valoración empleados.

Tabla 3 Niveles de valoración de activos informáticos

Nivel	Descripción
MA	Muy Alto
A	Alto
M	Medio
B	Bajo
MB	Muy Bajo

Fuente: el autor

La valoración de activos por dimensiones, tabla 4, establece la relevancia que para la empresa tiene cada activo informático en sus diferentes dimensiones.

Tabla 4 Valoración de los activos según sus dimensiones

ACTIVOS	DIMENSIONES				
	D	I	C	A	T
RED					
Router	M			M	M
Modem	M			M	M
HARDWARE					
Computadores	A	A	A	A	A
Impresoras Escáner y copiadoras	M				

UPS	M				
Servidor	MA	MA	MA	MA	MA
SOFTWARE					
Sistema Operativo		A	A	A	A
Software antivirus					M
Firewall					M
Ofimática					M
Correo electrónico		A	A	A	A
INFORMACIÓN					
Información Digital que se maneja en los diferentes medios indicados.		A	A		
Documentos físicos de información de todos los procesos de la empresa.	A	A	A	A	A
PERSONAL					
Gerente			M		
Subgerente			M		
Secretaria			M		
Médico ocupacional (3)			M		
Especialista en salud ocupacional (3)			M		
Mensajero			M		
Servicio externo de vigilancia			M		

Fuente el Autor

7.3 INVENTARIO DE ACTIVOS Y PROCESOS

El levantamiento del inventario de activos se ha realizado con la colaboración de la gerencia de la empresa dando acceso al registro de inventario.

Tabla 5 Listado Inventario de Activos y Procesos

IDENTIFICADOR				PROPIEDAD		LÍDER	ATRIBUTOS				CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN	
PROCESO Procesos Usomet	**AREA En la que se ejecuta el proceso**	**ACTIVO DE INFORMACIÓN Equipo informáticos que se usan en proceso**	**TIPO De equipo informático**	**PROPIETARIO Responsable de realizar el proceso**	**UBICACIÓN Dentro la empresa**	**NOMBRE PROPIETARIO Quien lidera el proceso**	**C**	**I**	**D**		**CLASIFICACIÓN**	**MISIONAL**
Realización del ciclo: Planear, Hacer, Verificar, Actuar	Gerencia	Portátil, Servidor, router, modem, medios electrónicos y físicos de almacenamiento	Comunicaciones, medios físicos, medios digitales, computadores, software, personal	Alba N. Sánchez C.	Gerencia	Alba N. Sánchez C.	MA	MA	A		A	Sí
Realización del ciclo: Planear, Hacer, Verificar, Actuar	Subgerencia	Portátil, Servidor, router, modem, medios electrónicos y físicos de almacenamiento	Comunicaciones, medios físicos, medios digitales, computadores, software, personal	Carlos A Tovar M.	Subgerencia	Alba N. Sánchez C.	A	A	A		A	Sí
Levantamiento de panorama de riesgos	Área Estudios de riesgos	Portátil, Servidor, router, modem, medios electrónicos y físicos de almacenamiento	Comunicaciones, medios físicos, medios digitales, computadores, software, personal	Carlos A Tovar M.	Área Estudios de riesgos	Alba N. Sánchez C.	A	A	A		A	Sí
Capacitación en gestión de riesgos industriales	Área de capacitación	Portátil, Servidor, router, modem, medios electrónicos y físicos de almacenamiento	Comunicaciones, medios físicos, medios digitales, computadores, software, personal	Carlos A Tovar M.	Área de capacitación	Alba N. Sánchez C.	M	M	M		M	Sí
Evaluación de salud ocupacional	Área médica ocupacional	Portátil, Servidor, router, modem, medios electrónicos y físicos de almacenamiento	Comunicaciones, medios físicos, medios digitales, computadores, software, personal	Germán Alfonso V.	Área médica ocupacional	Alba N. Sánchez C.	M	M	M		M	Sí
Gestión documental física, correspondencia física, trámites empresariales	Área de mensajería y archivo	Portátil, Servidor, router, modem, medios electrónicos y físicos de almacenamiento	Comunicaciones, medios físicos, medios digitales, computadores, software, personal	Carmen A Sánchez	Área de mensajería y archivo	Alba N. Sánchez C.	M	M	M		M	Sí

Fuente: el Autor

8. MEDIDAS DE SEGURIDAD

Se ha realizado un reconocimiento y evaluación de las medidas de seguridad existentes en la organización con los hallazgos descritos a continuación.

8.1 MEDIAS DE SEGURIDAD EXISTENTES

- Sin excepción los equipos de la infraestructura informática de la empresa solo pueden ser usados por personal autorizado.
- No está permitido descargar archivos a los equipos sin previa autorización.
- No está permitido extraer archivos con información de la empresa por cualquier medio sin previa autorización.
- El retiro de equipos de la empresa siempre debe ser previamente autorizado.
- Cada empleado debe realizar semanalmente copia de seguridad de la información en los equipos a su disposición.
- Se determinó que la empresa no cuenta con políticas de seguridad establecidas.

Es de resaltar que aparte de estas normas no hay en la empresa ninguna otra relacionada con la seguridad del sistema de información.

9. ANÁLISIS DE VULNERABILIDADES

Una vulnerabilidad definida como el estado de una debilidad que de ser explotada puede afectar la seguridad de los activos de la empresa.

Existen diferentes tipos de Vulnerabilidades, entre las cuales se mencionan:

- Natural: Se presentan principalmente en deficiencias, por ejemplo, no disponer de reguladores, no-Break, mal sistema de ventilación o calefacción[4].

- Física: Se refiere a la posibilidad de entrar o acceder físicamente al sistema para robar, modificar o destruirlo.

- Medios o Dispositivos: Se refiere a la posibilidad de robar o dañar los discos, cintas, listados de impresora, etc.

- Hardware: Fallas en las piezas físicas (ya sea por mal uso, descuido, mal diseño etc.) dejando al sistema desprotegido o inoperable.

- Software: Deficiencias en el funcionamiento del software. Ejemplo: controles de acceso, antivirus desactualizado, correos no deseados etc.

- Factor humano: Negligencia en el seguimiento de las políticas de seguridad, y mal uso del equipo de cómputo. Robo de información o la destrucción de los sistemas.

9.1 VALORACIÓN DE VULNERABILIDAD

En la tabla 7 se valoran las vulnerabilidades para establecer su prioridad, indicando la frecuencia de ocurrencia. Los posibles valores cuantitativos se indican en la tabla 6.

[4] RIESGOS Y CONTROL INFORMÁTICO, Lección 1, UNAD. Conceptos de Vulnerabilidad, Riesgos y Amenazas. Tomado el día 16 de marzo de 2016. [En línea] http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_1_conceptos_de_vulnerabilidad_riesgo_y_amenaza.html

Tabla 6 Matriz de Valoración de Vulnerabilidad por probabilidad de ocurrencia

Valor cuantitativo	Frecuencia	Descripción	Probabilidad
10	Muy Alta	A Diario	71 – 100%
8-9	Alta	Cada Semana	51 – 70%
5-7	Media	Cada Mes	31 % - 50 %
3-4	Bajo	Cada Año	11% - 30%
1-2	Muy Bajo	Cada varios años	0 -10 %

Fuente el autor

Tabla 7 Identificación y valoración de las vulnerabilidades

CATEGORÍA	ACTIVOS	VULNERABILIDADES	VALOR	PROBABILIDAD
COMUNICACIONES	• Router • Modem	Fallo en fluido eléctrico	4	30
		Exposición a líquidos	4	30
		Exposición a golpes	4	20
		Exposición a hurto	4	30
HARDWARE	• Computadores • Impresoras Escáner y copiadoras • UPS	Fallo en fluido eléctrico	4	30
		Exposición a líquidos	5	40
		Exposición a golpes	5	40
		Exposición a hurto	6	40
		Exposición a acceso indebido	4	40
SOFTWARE	• Sistema Operativo • Software antivirus • Firewall • Ofimática • Correo electrónico	Exposición a acceso indebido	6	50
		Exposición a virus	7	50
		Exposición a fallos de origen	7	50
Activos de Información Física	• Documentos físicos de información de	Exposición a líquidos	5	40

	todos los procesos de la empresa.	Exposición a golpes	5	40
		Exposición a hurto	6	40
		Exposición a acceso indebido	4	40
Activos de Información Digital	• Información Digital que se maneja en los diferentes medios indicados.	Fallo en fluido eléctrico	4	30
		Exposición a líquidos	5	40
		Exposición a golpes	5	40
		Exposición a hurto	6	40
		Exposición a acceso indebido	6	50
		Exposición a virus	7	50
		Exposición a fallos de origen	7	50
Recurso Humano	• Gerente • Subgerente • Secretaria • Médico ocupacional • Especialista en salud ocupacional • Mensajero • Servicio externo de vigilancia	Causar deterioro de la información por descuido	5	40
		Causar deterioro de la información intencionalmente	4	30
		Acceso no autorizado a determinada información.	4	30
		Hurto de información	4	30
		Dejar abierta la sesión sin vigilancia	7	50
		Descuidar o compartir usuario y clave de las aplicaciones.	4	30

Fuente el autor

.

10. GESTIÓN DEL RIESGO

10.1 IDENTIFICACIÓN DE LAS AMENAZAS

Las Amenazas están clasificadas en cuatro grupos las cuales son:

Tabla 8 Catálogo de Amenazas sobre los activos informáticos en MAGERIT.

TIPO DE AMENAZA	NOMENCLATURA	DEFINICIÓN
Desastres Naturales	**[N]**	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
De Origen Industrial	**[I]**	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
Errores y Fallos No Intencionados	**[E]**	Fallos no intencionales causados por las personas.
Ataques Intencionados	**[A]**	Fallos deliberados causados por las personas.

Fuente: AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos.

En la tabla 9 se identifican las amenazas naturales.

Tabla 9 Identificación amenazas de desastres naturales.

AMENAZA	DESCRIPCIÓN
[N] Fuego	Incendio: Posibilidad de que el fuego acabe con los recursos del sistema.
[N] Daños por Agua	Inundaciones: posibilidad de que el agua acabe con recursos informáticos.
[N]Desastres Naturales	Incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras.

Fuente: el autor

En la tabla 10 se identifican las amenazas de origen industrial.

Tabla 10 Identificación amenazas de origen industrial**.**

AMENAZA	DESCRIPCIÓN
[I] Contaminación Medioambiental.	Vibraciones, polvo, suciedad.
[I] Avería de origen Físico o lógico.	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
[I] Corte del suministro eléctrico.	Cese de la alimentación de potencia
[I] Condiciones inadecuadas de temperatura y/o humedad.	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad.
[I]Fallos de servicios de comunicación	Cese de la capacidad de transmitir datos de un sitio a otro.
[I] Degradación de los soportes de almacenamiento de la información.	Como consecuencia del paso del tiempo.

Fuente: el autor

En la tabla 11 se identifican las amenazas producidos por errores y fallos no intencionados.

Tabla 11 Identificación amenazas de errores y fallos no intencionados

AMENAZA	DESCRIPCIÓN
[E] Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.
[E] Errores mantenimiento y actualización de Software.	El administrador realiza mantenimiento y erróneamente realiza operaciones equivocadas.
[E] Errores de mantenimiento y actualización de Hardware.	Errores en los procedimientos de los procesos de actualización,
[E] Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas.
[E] Alteración accidental de la información	Alteración accidental de la información.
[E] Destrucción de información	Pérdida accidental de información.
[E] Divulgación de información.	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel.
[E]Caída del sistema por agotamiento de recursos.	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[E] Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público.

AMENAZA	DESCRIPCIÓN
[E] Errores de Administrador.	Son las equivocaciones que comenten los administradores a la hora de realizar una instalación u operación con el dispositivo.

Fuente: el autor

En la tabla 12 se identifican las amenazas por ataques intencionados.

Tabla 12 Identificación de amenazas de ataques intencionados

AMENAZAS	DESCRIPCIÓN
[A] Suplantación de la identidad del usuario.	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios.
[A] Abuso de privilegios de acceso.	Cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia hay problemas.
[A] Uso no previsto.	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales En internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.
[A] Daño por manipulación de usuario.	Falta de conciencia del buen uso de los equipos informáticos.
[A] Difusión de software dañino.	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
[A] Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin estar autorizado.
[A] Modificación de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.
[A] Destrucción la información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.
[A] Divulgación de información	Revelación de información.
[A] Manipulación de programas	Alteración intencionada del funcionamiento de los programas.
[A] Denegación de servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[A] Robo	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios es decir una indisponibilidad.
[A] Indisponibilidad del personal	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos.
[A] Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.
[A] Ingeniería social	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.

Fuente: www.udistrital.edu.co:8080/documents/276352/356568/Cap5GestionRiesgo.pdf

10.2 VALORACIÓN DE LAS AMENAZAS

Una vez determinadas las amenazas, se procede a valorar su influencia en el valor del activo, su objetivo es:

- Evaluar la probabilidad para saber cuán probable o improbable es que se materialice la amenaza.

- Estimar la degradación que causaría la amenaza en cada activo si llegara a materializarse, para saber cuán perjudicado resultaría el valor.

En la tabla 13 se indican los valores a asignar a las amenazas.

Tabla 13 Valor de amenazas

MA	MUY ALTA	5
A	ALTA	4
M	MEDIA	3
B	BAJA	2
MB	MUY BAJA	1

Fuente el Autor.

En la tabla 14 se indican los parámetros para la probabilidad de ocurrencia.

Tabla 14 Probabilidad de ocurrencia.

Valor cuantitativo	Frecuencia	Descripción	Probabilidad
5	Muy Alta	A Diario	80 – 100%
4	Alta	Cada Semana	50 – 70%
3	Media	Cada Mes	30 % - 50 %
2	Bajo	Cada Año	15% - 30%
1	Muy Bajo	Cada varios años	0 -10 %

Fuente el Autor

10.3 VALORACIÓN DEL IMPACTO

Debe describir como se calculará el impacto según MAGERIT.

IMPACTO = CONFIDENCIALIDAD X DISPONIBILIDAD X INTEGRIDAD (Redcom Ltda, 2009)

10.4 VALORACIÓN DE RIESGOS

El riesgo se valora como se indica en la tabla 15.

RIESGO = PROBABILIDAD X IMPACTO (Redcom Ltda, 2009)

Nota: Para la empresa las dimensiones de Autenticidad y Trazabilidad son de menor relevancia que las de Disponibilidad, Integridad y confidencialidad, en razón al pequeño tamaño de la empresa, por lo cual cada empleado tiene a cargo unos procesos específicos y cada proceso solo tiene un empleado asignado a su manejo. O sea, solo un empleado toca la información de cada proceso.

Tabla 15 Valoración de las amenazas, cálculo de impacto y riesgos

ACTIVOS	AMENAZAS	PROBA-BILIDAD	C	D	I	A	T	IMPACTO	RIESGOS
RED									
Router	[N] Fuego	4	2	2	3	1	1	12	48
	[N] Daños por Agua	4	2	2	3	1	1	12	48
	[N]Desastres Naturales	4	2	2	2	1	1	8	32
	[I] Avería de origen Físico o lógico.	4	2	5	5	1	1	50	200
	[I] Corte del suministro eléctrico.	4	2	5	2	1	1	20	80
	[I] Condiciones inadecuadas de temperatura y/o humedad.	4	2	2	2	1	1	8	32
	[I]Fallos de servicios de comunicación	4	2	5	2	1	1	20	80
	[A] Uso no previsto.	4	2	5	2	1	1	20	80
	[A] Daño por manipulación de usuario.	4	2	2	2	1	1	8	32
	[A] Acceso no autorizado	4	2	5	2	1	1	20	80
	[A] Modificación de la información	4	2	2	2	1	1	8	32
	[A] Robo	4	3	2	3	1	1	18	72

ACTIVOS	AMENAZAS	PROBA-BILIDAD	C	D	I	A	T	IMPACTO	RIESGOS
Modem	[N] Fuego	4	2	2	2	1	1	8	32
	[N] Daños por Agua	4	3	2	3	1	1	18	72
	[N]Desastres Naturales	4	2	2	2	1	1	8	32
	[I] Avería de origen Físico o lógico.	4	2	5	5	1	1	50	200
	[I] Corte del suministro eléctrico.	4	2	5	2	1	1	20	80
	[I] Condiciones inadecuadas de temperatura y/o humedad.	4	2	2	2	1	1	8	32
	[I]Fallos de servicios de comunicación	4	2	5	2	1	1	20	80
	[A] Uso no previsto.	4	2	5	2	1	1	20	80
	[A] Daño por manipulación de usuario.	4	2	2	2	1	1	8	32
	[A] Acceso no autorizado	4	2	5	2	1	1	20	80
	[A] Modificación de la información	4	2	2	2	1	1	8	32
	[A] Robo	4	2	2	2	1	1	8	32
HARDWARE									
Computadores	[N] Fuego	4	3	2	5	1	1	30	120

ACTIVOS	AMENAZAS	PROBA-BILIDAD	C	D	I	A	T	IMPACTO	RIESGOS
	[N] Daños por Agua	4	3	2	3	1	1	18	72
	[N]Desastres Naturales	4	2	2	2	1	1	8	32
	[I] Avería de origen Físico o lógico.	4	3	2	2	1	1	12	48
	[I] Corte del suministro eléctrico.	4	3	2	2	1	1	12	48
	[I] Condiciones inadecuadas de temperatura y/o humedad.	4	2	2	2	1	1	8	32
	[I]Fallos de servicios de comunicación	4	3	2	3	1	1	18	72
	[I] Degradación de los soportes de almacenamiento de la información.	4	3	2	2	1	1	12	48
	[E] Errores de los usuarios	4	3	2	2	1	1	12	48
	[E] Errores mantenimiento y actualización de Software.	5	3	5	5	1	1	75	375
	[E] Errores de mantenimiento y actualización de Hardware.	4	4	2	3	1	1	24	96
	[E] Difusión de software dañino	4	3	2	5	1	1	30	120
	[E] Alteración accidental de la información	4	3	2	2	1	1	12	48
	[E]Caída del sistema por agotamiento de recursos.	4	2	2	3	1	1	12	48
	[E] Errores de Administrador.	4	2	2	3	1	1	12	48

ACTIVOS	AMENAZAS	PROBA-BILIDAD	C	D	I	A	T	IMPACTO	RIESGOS
	[A] Suplantación de la identidad del usuario.	4	3	2	5	1	1	30	120
	[A] Abuso de privilegios de acceso.	4	2	2	5	1	1	20	80
	[A] Uso no previsto.	4	3	2	5	1	1	30	120
	[A] Daño por manipulación de usuario.	4	4	2	5	1	1	40	160
	[A] Acceso no autorizado	4	3	2	5	1	1	30	120
	[A] Modificación de la información	4	5	2	5	1	1	50	200
	[A] Destrucción la información	4	4	2	5	1	1	40	160
	[A] Divulgación de información	4	5	5	3	1	1	75	300
	[A] Manipulación de programas	4	3	2	3	1	1	18	72
	[A] Denegación de servicio	4	3	2	3	1	1	18	72
	[A] Robo	4	3	2	3	1	1	18	72
Impresoras Escáner y copiadoras	[N] Fuego	4	2	2	2	1	1	8	32
	[N] Daños por Agua	4	2	2	2	1	1	8	32
	[N]Desastres Naturales	4	2	2	2	1	1	8	32

ACTIVOS	AMENAZAS	PROBA-BILIDAD	C	D	I	A	T	IMPACTO	RIESGOS
	[I] Avería de origen Físico o lógico.	4	2	2	2	1	1	8	32
	[I] Corte del suministro eléctrico.	4	2	2	2	1	1	8	32
	[I] Condiciones inadecuadas de temperatura y/o humedad.	4	2	2	2	1	1	8	32
	[I]Fallos de servicios de comunicación	4	2	2	2	1	1	8	32
	[A] Uso no previsto.	4	2	2	2	1	1	8	32
	[A] Daño por manipulación de usuario.	4	2	2	2	1	1	8	32
	[A] Acceso no autorizado	4	2	2	2	1	1	8	32
	[A] Modificación de la información	4	2	2	2	1	1	8	32
	[A] Robo	4	2	2	2	1	1	8	32
UPS	[N] Fuego	4	2	2	2	1	1	8	32
	[N] Daños por Agua	4	2	2	2	1	1	8	32
	[N]Desastres Naturales	4	2	2	2	1	1	8	32
	[I] Avería de origen Físico o lógico.	4	2	2	2	1	1	8	32
	[I] Corte del suministro eléctrico.	4	2	2	2	1	1	8	32

ACTIVOS	AMENAZAS	PROBA-BILIDAD	C	D	I	A	T	IMPACTO	RIESGOS
	[I] Condiciones inadecuadas de temperatura y/o humedad.	4	2	2	2	1	1	8	32
	[I]Fallos de servicios de comunicación	4	2	2	2	1	1	8	32
	[A] Uso no previsto.	4	2	2	2	1	1	8	32
	[A] Daño por manipulación de usuario.	4	2	2	2	1	1	8	32
	[A] Acceso no autorizado	4	2	2	2	1	1	8	32
	[A] Modificación de la información	4	2	2	2	1	1	8	32
	[A] Robo	4	2	2	2	1	1	8	32
Servidor	[N] Fuego	4	4	2	5	1	1	40	160
	[N] Daños por Agua	4	4	2	4	1	1	32	128
	[N]Desastres Naturales	4	2	2	2	1	1	8	32
	[I] Avería de origen Físico o lógico.	4	3	4	3	1	1	36	144
	[I] Corte del suministro eléctrico.	4	3	3	3	1	1	27	108
	[I] Condiciones inadecuadas de temperatura y/o humedad.	4	2	2	2	1	1	8	32
	[I]Fallos de servicios de comunicación	4	3	2	2	1	1	12	48

ACTIVOS	AMENAZAS	PROBA-BILIDAD	C	D	I	A	T	IMPACTO	RIESGOS
	[I] Degradación de los soportes de almacenamiento de la información.	4	2	2	2	1	1	8	32
	[E] Errores de los usuarios	4	2	2	2	1	1	8	32
	[E] Errores mantenimiento y actualización de Software.	5	2	5	5	1	1	50	250
	[E] Errores de mantenimiento y actualización de Hardware.	4	2	2	2	1	1	8	32
	[E] Difusión de software dañino	4	3	2	5	1	1	30	120
	[E] Alteración accidental de la información	4	3	2	2	1	1	12	48
	[E] Divulgación de información.	4	5	2	4	1	1	40	160
	[E]Caída del sistema por agotamiento de recursos.	4	2	2	2	1	1	8	32
	[E] Errores de Administrador.	4	2	2	1	1	1	4	16
	[A] Suplantación de la identidad del usuario.	4	2	2	5	1	1	20	80
	[A] Abuso de privilegios de acceso.	4	3	2	5	1	1	30	120
	[A] Uso no previsto.	4	2	2	5	1	1	20	80
	[A] Daño por manipulación de usuario.	4	2	2	5	1	1	20	80
	[A] Acceso no autorizado	4	3	2	5	1	1	30	120

ACTIVOS	AMENAZAS	PROBA-BILIDAD	C	D	I	A	T	IMPACTO	RIESGOS
	[A] Modificación de la información	4	5	2	5	1	1	50	200
	[A] Destrucción la información	4	3	2	5	1	1	30	120
	[A] Manipulación de programas	4	2	2	2	1	1	8	32
	[A] Denegación de servicio	4	2	2	2	1	1	8	32
	[A] Robo	4	2	2	2	1	1	8	32
SOFTWARE									
Sistema Operativo	[I] Avería de origen Físico o lógico.	4	2	2	3	1	1	12	48
	[I] Corte del suministro eléctrico.	4	2	2	2	1	1	8	32
	[I] Degradación de los soportes de almacenamiento de la información.	4	2	2	2	1	1	8	32
	[E] Errores de los usuarios	4	2	2	2	1	1	8	32
	[E] Errores mantenimiento y actualización de Software.	5	2	5	5	1	1	50	250
	[E] Difusión de software dañino	4	2	2	5	1	1	20	80
	[E]Caída del sistema por agotamiento de recursos.	4	2	2	2	1	1	8	32

ACTIVOS	AMENAZAS	PROBA-BILIDAD	C	D	I	A	T	IMPACTO	RIESGOS
	[E] Errores de Administrador.	4	2	2	2	1	1	8	32
	[A] Suplantación de la identidad del usuario.	4	2	2	5	1	1	20	80
	[A] Abuso de privilegios de acceso.	4	2	2	5	1	1	20	80
	[A] Uso no previsto.	4	2	2	5	1	1	20	80
	[A] Daño por manipulación de usuario.	4	2	2	5	1	1	20	80
	[A] Acceso no autorizado	4	2	2	5	1	1	20	80
	[A] Manipulación de programas	4	3	2	2	1	1	12	48
	[A] Denegación de servicio	4	2	2	2	1	1	8	32
	[E]Caída del sistema por agotamiento de recursos.	4	2	4	2	1	1	16	64
Software antivirus	[I] Avería de origen Físico o lógico.	4	2	2	3	1	1	12	48
	[I] Corte del suministro eléctrico.	4	3	2	3	1	1	18	72
	[I] Degradación de los soportes de almacenamiento de la información.	4	3	2	2	1	1	12	48
	[E] Errores de los usuarios	4	3	2	2	1	1	12	48
	[E] Errores mantenimiento y actualización de Software.	5	3	5	5	1	1	75	375

ACTIVOS	AMENAZAS	PROBA-BILIDAD	C	D	I	A	T	IMPACTO	RIESGOS
	[E] Difusión de software dañino	4	3	2	5	1	1	30	120
	[E]Caída del sistema por agotamiento de recursos.	4	3	2	2	1	1	12	48
	[E] Errores de Administrador.	4	2	2	2	1	1	8	32
	[A] Suplantación de la identidad del usuario.	4	2	2	5	1	1	20	80
	[A] Abuso de privilegios de acceso.	4	2	2	5	1	1	20	80
	[A] Uso no previsto.	4	2	2	5	1	1	20	80
	[A] Daño por manipulación de usuario.	4	2	2	5	1	1	20	80
	[A] Acceso no autorizado	4	3	2	5	1	1	30	120
	[A] Manipulación de programas	4	2	2	2	1	1	8	32
	[A] Denegación de servicio	4	2	2	3	1	1	12	48
Firewall	[I] Avería de origen Físico o lógico.	4	3	2	2	1	1	12	48
	[I] Corte del suministro eléctrico.	4	2	2	3	1	1	12	48
	[I] Degradación de los soportes de almacenamiento de la información.	4	2	2	1	1	1	4	16
	[E] Errores de los usuarios	4	2	2	2	1	1	8	32

ACTIVOS	AMENAZAS	PROBA-BILIDAD	C	D	I	A	T	IMPACTO	RIESGOS
	[E] Errores mantenimiento y actualización de Software.	5	2	5	5	1	1	50	250
	[E] Difusión de software dañino	4	3	2	5	1	1	30	120
	[E]Caída del sistema por agotamiento de recursos.	4	3	2	1	1	1	6	24
	[E] Errores de Administrador.	4	3	2	1	1	1	6	24
	[A] Suplantación de la identidad del usuario.	4	3	2	5	1	1	30	120
	[A] Abuso de privilegios de acceso.	4	2	2	5	1	1	20	80
	[A] Uso no previsto.	4	3	2	5	1	1	30	120
	[A] Daño por manipulación de usuario.	4	2	2	5	1	1	20	80
	[A] Acceso no autorizado	4	2	2	5	1	1	20	80
	[A] Manipulación de programas	4	2	2	3	1	1	12	48
	[A] Denegación de servicio	4	2	2	2	1	1	8	32
Ofimática	[I] Avería de origen Físico o lógico.	4	2	2	2	1	1	8	32
	[I] Corte del suministro eléctrico.	4	3	2	3	1	1	18	72
	[I] Degradación de los soportes de almacenamiento de la información.	4	2	2	2	1	1	8	32

ACTIVOS	AMENAZAS	PROBA-BILIDAD	C	D	I	A	T	IMPACTO	RIESGOS
	[E] Errores de los usuarios	4	2	2	2	1	1	8	32
	[E] Errores mantenimiento y actualización de Software.	5	2	5	5	1	1	50	250
	[E] Difusión de software dañino	4	3	2	5	1	1	30	120
	[E]Caída del sistema por agotamiento de recursos.	4	2	2	2	1	1	8	32
	[E] Errores de Administrador.	4	2	2	2	1	1	8	32
	[A] Suplantación de la identidad del usuario.	4	2	2	5	1	1	20	80
	[A] Abuso de privilegios de acceso.	4	2	2	5	1	1	20	80
	[A] Uso no previsto.	4	2	2	5	1	1	20	80
	[A] Daño por manipulación de usuario.	4	2	2	5	1	1	20	80
	[A] Acceso no autorizado	4	3	2	5	1	1	30	120
	[A] Manipulación de programas	4	3	2	3	1	1	18	72
	[A] Denegación de servicio	4	3	2	3	1	1	18	72
Correo electrónico	[I] Avería de origen Físico o lógico.	4	3	2	3	1	1	18	72
	[I] Corte del suministro eléctrico.	4	3	2	3	1	1	18	72

ACTIVOS	AMENAZAS	PROBA-BILIDAD	C	D	I	A	T	IMPACTO	RIESGOS
	[I] Degradación de los soportes de almacenamiento de la información.	4	3	2	3	1	1	18	72
	[E] Errores de los usuarios	4	3	2	2	1	1	12	48
	[E] Errores mantenimiento y actualización de Software.	5	3	5	5	1	1	75	375
	[E] Difusión de software dañino	4	3	2	5	1	1	30	120
	[E]Caída del sistema por agotamiento de recursos.	4	3	2	3	1	1	18	72
	[E] Errores de Administrador.	4	3	2	3	1	1	18	72
	[A] Suplantación de la identidad del usuario.	4	3	2	5	1	1	30	120
	[A] Abuso de privilegios de acceso.	4	3	2	5	1	1	30	120
	[A] Uso no previsto.	4	3	2	5	1	1	30	120
	[A] Daño por manipulación de usuario.	4	3	2	5	1	1	30	120
	[A] Acceso no autorizado	4	3	2	5	1	1	30	120
	[A] Manipulación de programas	4	3	2	1	1	1	6	24
	[A] Denegación de servicio	4	3	2	3	1	1	18	72
INFORMACIÓN									

ACTIVOS	AMENAZAS	PROBA-BILIDAD	C	D	I	A	T	IMPACTO	RIESGOS
Documentos	[N] Fuego	4	2	5	3	1	1	30	120
	[N] Daños por Agua	4	2	5	3	1	1	30	120
	[N]Desastres Naturales	4	2	5	3	1	1	30	120
	[I] Avería de origen Físico o lógico.	4	2	5	3	1	1	30	120
	[I] Degradación de los soportes de almacenamiento de la información.	4	2	2	3	1	1	12	48
	[E] Errores de los usuarios	4	4	4	3	1	1	48	192
	[E] Destrucción de información	4	3	5	3	1	1	45	180
	[A] Uso no previsto.	4	4	4	3	1	1	48	192
	[A] Daño por manipulación de usuario.	4	2	2	3	1	1	12	48
	[A] Acceso no autorizado	4	2	2	3	1	1	12	48
	[A] Divulgación de información	4	5	3	3	1	1	45	180
	[A] Robo	4	5	5	3	1	1	75	300
Información Digital	[N] Fuego	4	3	2	5	1	1	30	120
	[N] Daños por Agua	4	3	2	3	1	1	18	72

ACTIVOS	AMENAZAS	PROBA-BILIDAD	C	D	I	A	T	IMPACTO	RIESGOS
	[N]Desastres Naturales	4	3	2	3	1	1	18	72
	[I] Avería de origen Físico o lógico.	4	3	2	3	1	1	18	72
	[I] Corte del suministro eléctrico.	4	4	4	4	1	1	64	256
	[I] Condiciones inadecuadas de temperatura y/o humedad.	4	3	2	3	1	1	18	72
	[I]Fallos de servicios de comunicación	4	3	2	3	1	1	18	72
	[I] Degradación de los soportes de almacenamiento de la información.	4	3	2	3	1	1	18	72
	[E] Errores de los usuarios	5	3	5	3	1	1	45	225
	[E] Errores mantenimiento y actualización de Software.	5	4	4	4	1	1	64	320
	[E] Difusión de software dañino	4	3	2	5	1	1	30	120
	[E] Alteración accidental de la información	4	3	2	2	1	1	12	48
	[E] Errores de Administrador.	4	3	2	3	1	1	18	72
	[A] Abuso de privilegios de acceso.	4	5	2	5	1	1	50	200
	[A] Uso no previsto.	4	3	2	5	1	1	30	120

ACTIVOS	AMENAZAS	PROBA-BILIDAD	C	D	I	A	T	IMPACTO	RIESGOS
	[A] Daño por manipulación de usuario.	4	3	2	5	1	1	30	120
	[A] Acceso no autorizado	4	3	2	5	1	1	30	120
	[A] Modificación de la información	5	5	5	5	1	1	125	625
	[A] Destrucción la información	4	5	5	5	1	1	125	500
	[A] Divulgación de información	5	4	4	4	1	1	64	320
	[A] Robo	4	5	5	5	1	1	125	500
PERSONAL									
Personal	[E] Errores de los usuarios	5	3	5	3	1	1	45	225
	[A] Suplantación de la identidad del usuario.	5	5	3	3	1	1	45	225
	[A] Ingeniería social	4	5	5	5	1	1	125	500
	[A] Extorsión	4	5	5	5	1	1	125	500
	[A] Indisponibilidad del personal	4	5	5	5	1	1	125	500

Fuente: El autor

10.5 NIVEL DE LOS RIESGOS

En la tabla 17 se clasifican los riesgos de acuerdo a su nivel y en la tabla 18 se evalúan.

Tabla 16 Niveles de riesgos

NIVEL DE RIESGO				
BAJO ≤125	**MEDIO >125 y ≤250**	**ALTO >250 y ≤ 375**	**MUY ALTO >375 y ≤ 500**	**CRITICO >500 y ≤ 625**

Fuente: El autor.

Tabla 17 Nivel de riesgo

ACTIVOS	AMENAZAS	Bajo	Medio	Alto	Muy Alto	Critico
RED						
Router	[N] Fuego					
	[N] Daños por Agua					
	[N]Desastres Naturales					
	[I] Avería de origen Físico o lógico.					

	[I] Corte del suministro eléctrico.					
	[I] Condiciones inadecuadas de temperatura y/o humedad.					
	[I]Fallos de servicios de comunicación					
	[A] Uso no previsto.					
	[A] Daño por manipulación de usuario.					
	[A] Acceso no autorizado					
	[A] Modificación de la información					
	[A] Robo					
Modem	[N] Fuego					
	[N] Daños por Agua					
	[N]Desastres Naturales					
	[I] Avería de origen Físico o lógico.					
	[I] Corte del suministro eléctrico.					

	[I] Condiciones inadecuadas de temperatura y/o humedad.					
	[I]Fallos de servicios de comunicación					
	[A] Uso no previsto.					
	[A] Daño por manipulación de usuario.					
	[A] Acceso no autorizado					
	[A] Modificación de la información					
	[A] Robo					
HARDWARE						
Computadores	[N] Fuego					
	[N] Daños por Agua					
	[N]Desastres Naturales					
	[I] Avería de origen					
	Físico o lógico.					
	[I] Corte del suministro eléctrico.					

	[I] Condiciones inadecuadas de temperatura y/o humedad.					
	[I]Fallos de servicios de comunicación					
	[I] Degradación de los soportes de almacenamiento de la información.					
	[E] Errores de los usuarios					
	[E] Errores mantenimiento y actualización de Software.					
	[E] Errores de mantenimiento y actualización de Hardware.					
	[E] Difusión de software dañino					
	[E] Alteración accidental de la información					
	[E]Caída del sistema por agotamiento de recursos.					
	[E] Errores de Administrador.					

	[A] Suplantación de la identidad del usuario.					
	[A] Abuso de privilegios de acceso.					
	[A] Uso no previsto.					
	[A] Daño por manipulación de usuario.					
	[A] Acceso no autorizado					
	[A] Modificación de la información					
	[A] Destrucción la información					
	[A] Divulgación de información					
	[A] Manipulación de programas					
	[A] Denegación de servicio					
	[A] Robo					
Impresoras Escáner y copiadoras	[N] Fuego					
	[N] Daños por Agua					
	[N]Desastres Naturales					
	[I] Avería de origen Físico o lógico.					

	[I] Corte del suministro eléctrico.					
	[I] Condiciones inadecuadas de temperatura y/o humedad.					
	[I]Fallos de servicios de comunicación					
	[A] Uso no previsto.					
	[A] Daño por manipulación de usuario.					
	[A] Acceso no autorizado					
	[A] Modificación de la información					
	[A] Robo					
UPS	[N] Fuego					
	[N] Daños por Agua					
	[N]Desastres Naturales					
	[I] Avería de origen Físico o lógico.					
	[I] Corte del suministro eléctrico.					

	[I] Condiciones inadecuadas de temperatura y/o humedad.					
	[I]Fallos de servicios de comunicación					
	[A] Uso no previsto.					
	[A] Daño por manipulación de usuario.					
	[A] Acceso no autorizado					
	[A] Modificación de la información					
	[A] Robo					
Servidor	[N] Fuego					
	[N] Daños por Agua					
	[N]Desastres Naturales					
	[I] Avería de origen Físico o lógico.					
	[I] Corte del suministro eléctrico.					
	[I] Condiciones inadecuadas de temperatura y/o humedad.					

	[I]Fallos de servicios de comunicación					
	[I] Degradación de los soportes de almacenamiento de la información.					
	[E] Errores de los usuarios					
	[E] Errores mantenimiento y actualización de Software.					
	[E] Errores de mantenimiento y actualización de Hardware.					
	[E] Difusión de software dañino					
	[E] Alteración accidental de la información					
	[E] Divulgación de información.					
	[E]Caída del sistema por agotamiento de recursos.					
	[E] Errores de Administrador.					
	[A] Suplantación de la identidad del usuario.					

	[A] Abuso de privilegios de acceso.					
	[A] Uso no previsto.					
	[A] Daño por manipulación de usuario.					
	[A] Acceso no autorizado					
	[A] Modificación de la información					
	[A] Destrucción la información					
	[A] Divulgación de información					
	[A] Manipulación de programas					
	[A] Denegación de servicio					
	[A] Robo					
SOFTWARE						
Sistema Operativo	[I] Avería de origen Físico o lógico.					
	[I] Corte del suministro eléctrico.					

	[I] Degradación de los soportes de almacenamiento de la información.					
	[E] Errores de los usuarios					
	[E] Errores mantenimiento y actualización de Software.					
	[E] Difusión de software dañino					
	[E]Caída del sistema por agotamiento de recursos.					
	[E] Errores de Administrador.					
	[A] Suplantación de la identidad del usuario.					
	[A] Abuso de privilegios de acceso.					
	[A] Uso no previsto.					
	[A] Daño por manipulación de usuario.					
	[A] Acceso no autorizado					

	[A] Manipulación de programas					
	[A] Denegación de servicio					
	[E]Caída del sistema por agotamiento de recursos.					
Software antivirus	[I] Avería de origen Físico o lógico.					
	[I] Corte del suministro eléctrico.					
	[I] Degradación de los soportes de almacenamiento de la información.					
	[E] Errores de los usuarios					
	[E] Errores mantenimiento y actualización de Software.					
	[E] Difusión de software dañino					
	[E]Caída del sistema por agotamiento de recursos.					
	[E] Errores de Administrador.					

	[A] Suplantación de la identidad del usuario.					
	[A] Abuso de privilegios de acceso.					
	[A] Uso no previsto.					
	[A] Daño por manipulación de usuario.					
	[A] Acceso no autorizado					
	[A] Manipulación de programas					
	[A] Denegación de servicio					
Firewall	[I] Avería de origen Físico o lógico.					
	[I] Corte del suministro eléctrico.					
	[I] Degradación de los soportes de almacenamiento de la información.					
	[E] Errores de los usuarios					
	[E] Errores mantenimiento y actualización de Software.					

	[E] Difusión de software dañino					
	[E]Caída del sistema por agotamiento de recursos.					
	[E] Errores de Administrador.					
	[A] Suplantación de la identidad del usuario.					
	[A] Abuso de privilegios de acceso.					
	[A] Uso no previsto.					
	[A] Daño por manipulación de usuario.					
	[A] Acceso no autorizado					
	[A] Manipulación de programas					
	[A] Denegación de servicio					
Ofimática	[I] Avería de origen Físico o lógico.					
	[I] Corte del suministro eléctrico.					

	[I] Degradación de los soportes de almacenamiento de la información.					
	[E] Errores de los usuarios					
	[E] Errores mantenimiento y actualización de Software.					
	[E] Difusión de software dañino					
	[E]Caída del sistema por agotamiento de recursos.					
	[E] Errores de Administrador.					
	[A] Suplantación de la identidad del usuario.					
	[A] Abuso de privilegios de acceso.					
	[A] Uso no previsto.					
	[A] Daño por manipulación de usuario.					
	[A] Acceso no autorizado					

	[A] Manipulación de programas					
	[A] Denegación de servicio					
Correo electrónico	[I] Avería de origen Físico o lógico.					
	[I] Corte del suministro eléctrico.					
	[I] Degradación de los soportes de almacenamiento de la información.					
	[E] Errores de los usuarios					
	[E] Errores mantenimiento y actualización de Software.					
	[E] Difusión de software dañino					
	[E]Caída del sistema por agotamiento de recursos.					
	[E] Errores de Administrador.					
	[A] Suplantación de la identidad del usuario.					

	[A] Abuso de privilegios de acceso.					
	[A] Uso no previsto.					
	[A] Daño por manipulación de usuario.					
	[A] Acceso no autorizado					
	[A] Manipulación de programas					
	[A] Denegación de servicio					
INFORMACIÓN						
Documentos	[N] Fuego					
	[N] Daños por Agua					
	[N]Desastres Naturales					
	[I] Avería de origen Físico o lógico.					
	[I] Degradación de los soportes de almacenamiento de la información.					
	[E] Errores de los usuarios					
	[E] Destrucción de información					

	[A] Uso no previsto.					
	[A] Daño por manipulación de usuario.					
	[A] Acceso no autorizado					
	[A] Divulgación de información					
	[A] Robo					
Información Digital	[N] Fuego					
	[N] Daños por Agua					
	[N]Desastres Naturales					
	[I] Avería de origen Físico o lógico.					
	[I] Corte del suministro eléctrico.					
	[I] Condiciones inadecuadas de temperatura y/o humedad.					
	[I]Fallos de servicios de comunicación					

	[I] Degradación de los soportes de almacenamiento de la información.					
	[E] Errores de los usuarios					
	[E] Errores mantenimiento y actualización de Software.					
	[E] Difusión de software dañino					
	[E] Alteración accidental de la información					
	[E] Errores de Administrador.					
	[A] Abuso de privilegios de acceso.					
	[A] Uso no previsto.					
	[A] Daño por manipulación de usuario.					
	[A] Acceso no autorizado					
	[A] Modificación de la información					
	[A] Destrucción la información					

	[A] Divulgación de información					
	[A] Robo					
PERSONAL						
PERSONAL	[E] Errores de los usuarios					
	[A] Suplantación de la identidad del usuario					
	[A] Ingeniería social					
	[A] Extorsión					
	[A] Indisponibilidad del personal					

Fuente: El autor.

10.6 TRATAMIENTO DE LOS RIESGOS

Debido a que el plan de tratamiento de riesgos está indicado en la normativa ISO/IEC 27001:2013 y es de estricto cumplimiento se debe elaborar el plan con base en la normativa ISO/IEC 27002 numeral 4, Evaluación y tratamiento del riesgo.

Imagen 3 Numeral 4 de la norma ISO/IEC 27002

Ref.	Objetivo	Consejo de implementación	Posibles métricas
4. Evaluación y tratamiento de riesgos			
4.1	Evaluación de riesgos de seguridad	Aplicar los métodos de gestión de seguridad de la información, con preferencia por métodos documentados y estructurados como: OCTABE, MEHARI, ISO TR 13335 O BS 7799 parte 3 (y en su momento, ISO/IEC 27005.	Porcentaje de riesgos evaluados como de importancia alta, media o baja.
4.2	Tratamiento de riesgos de seguridad	La gerencia evaluará los riesgos analizando su manejo. Sin embargo, toda decisión debe ser documentada. La gerencia también determinará el margen de tolerancia al riesgo en la organización.	Proyección de riesgos de la información conforme su relevancia. Medición de la eficacia y eficiencia en el manejo del presupuesto de seguridad.

Fuente: ISO27000.es. Consejos de implantación y métricas de ISO/IEC 27001 y 27002. 2007. Tomado de: http://www.iso27000.es/download/ISO_27000_implementation_guidance_v1_Spanish.pdf

Tabla 18 Tratamiento de los riesgos

ACTIVOS	AMENAZAS	IMPACTO	Tratamiento del Riesgo	Área Afectada
HARDWARE				
Computadores	[E] Errores mantenimiento y actualización de Hardware.	75	Se deben establecer directivas que permitan mantener los equipos en buen estado, y con ello asegurar su disponibilidad para llevar a cabo las tareas de procesamiento y almacenamiento de información.	Toda la empresa
	[A] Divulgación de información.	75	Las instalaciones y la información que se genera se deben proteger contra cualquier alteración y acceso no autorizado.	Toda la empresa
SOFTWARE				
Software antivirus	[E] Errores mantenimiento y actualización de Software.	75	Es necesario incluir los requerimientos de controles de seguridad en las especificaciones técnicas de todo nuevo sistema de información, modificación y/o ampliación de los existentes.	Toda la empresa
Correo electrónico	[E] Errores mantenimiento y actualización de Software.	75	Es necesario incluir los requerimientos de controles de seguridad en las especificaciones técnicas de todo nuevo sistema de información, modificación y/o ampliación de los existentes.	Toda la empresa

ACTIVOS	AMENAZAS	IMPACTO	Tratamiento del Riesgo	Área Afectada
INFORMACIÓN				
Documentos	[A] Robo	75	Se requiere mantener un contacto con las autoridades competentes para estar al día con las últimas noticias relacionados con ataques a sistemas de información. También para reportar los posibles incidentes que se puedan presentar en la entidad y requieran la investigación y judicialización de personas.	Toda la empresa
Información Digital	[I] Corte del suministro eléctrico.	64	Se deben implementar sistemas con UPS y generadores de Backups, con verificación periódica de buen funcionamiento y registro en bitácora.	Toda la empresa
	[E] Errores mantenimiento y actualización de Software.	64	Es necesario incluir los requerimientos de controles de seguridad en las especificaciones técnicas de todo nuevo sistema de información, modificación y/o ampliación de los existentes.	Toda la empresa
	[A] Modificación de la información	125	La empresa debe llevar a cabo evaluaciones periódicas del riesgo y la magnitud del daño que puede resultar en el acceso no autorizado, uso, revelación, alteración, modificación o destrucción de información y sistemas de información que soportan las operaciones y activos de la empresa, tomar los correctivos pertinentes y divulgar la política que se genere.	Toda la empresa
	[A] Destrucción la información	125	La empresa debe llevar a cabo evaluaciones periódicas del riesgo y la magnitud del daño que se puede generar por destrucción de información y sistemas de información que soportan las operaciones y activos de la empresa para tomar los correctivos pertinentes y divulgar la política que se genere.	Toda la empresa

ACTIVOS	AMENAZAS	IMPACTO	Tratamiento del Riesgo	Área Afectada
	[A] Divulgación de información	64	Protección de la información de registro; Las instalaciones y la información que se genera se deben proteger contra alteración y acceso no autorizado.	Toda la empresa
	[A] Robo	125	Es necesario mantener un contacto con las autoridades competentes para estar al día con las últimas noticias relacionados con ataques a sistemas de información. También para reportar los posibles incidentes que se puedan presentar en la entidad y requieran la investigación y judicialización de personas.	Toda la empresa
PERSONAL				
PERSONAL	[E] Errores de los usuarios	225	Se requiere realizar en forma periódica capacitaciones a usuarios, revisando en especial loe puntos en los que con mayor frecuencia se presenten errores.	Toda la empresa
	[A] Suplantación de la identidad del usuario	225	Es indispensable establecer procedimiento de aplicación permanente que permitan cotejar la identidad de los usuarios.	Toda la empresa

ACTIVOS	AMENAZAS	IMPACTO	Tratamiento del Riesgo	Área Afectada
	[A] Ingeniería social	500	Periódicamente debe realizarse capacitación a los usuarios para que conozcan cómo no ser víctimas de las nuevas modalidades de ingeniería social.	Toda la empresa
	[A] Extorsión	500	Se requiere mantener un contacto con las autoridades competentes para estar al día en las novedades relacionados con las nuevas modalidades de extorsión.	Toda la empresa
	[A] Indisponibilidad del personal	500	Se requiere mantener identificado el personal que puede suplir las labores de sus compañeros en caso de indisponibilidad, lo cual hace necesario que también conozca sobre sus responsabilidades.	Toda la empresa

Fuente: El autor

10.7 OBJETIVOS DE CONTROL

Para establecer los objetivos de control, tabla 20, se realizó el análisis de cada riesgo y con apoyo de la norma ISO/IEC 27002:2013 que cuenta con 14 dominios, 35 objetivos de control y 114 controles.

Tabla 19 Asignación de controles a cada riesgo

RIESGOS	OBJETIVOS DE CONTROL	CONTROLES	DEFINICIÓN DEL CONTROL
HARDWARE Computadores			
Errores mantenimiento y actualización de Hardware.	09. Seguridad Física y del Entorno. 9 2 Seguridad de los equipos 9.2.4. Mantenimiento de equipos	Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.	Mantener actualizado el Registro de los proveedores de cada elemento hardware en uso sistema, para facilitar el contacto inmediato en caso de requerir mantenimiento correctivo. Llevar bitácora de mantenimiento preventivo y correctivo para cada equipo.
Divulgación de información.	09. Seguridad Física y del Entorno. 9 2 Seguridad de los equipos 9.2.4. Mantenimiento de equipos	Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.	Mantener actualizado el Registro de proveedores de cada elemento hardware adquirido para el sistema, de forma que facilite el contacto en caso de requerir mantenimiento correctivo. Llevar bitácora de mantenimiento preventivo y correctivo para cada equipo.
SOFTWARE Software antivirus Correo electrónico			
Errores mantenimiento y actualización de Software.	12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información. 12 1 Requisitos de seguridad de los sistemas. 12.1.1. Análisis y especificación de los requisitos de seguridad.	Las demandas de nuevos sistemas de información para el negocio o mejoras de los sistemas ya existentes deberían especificar los Requisitos de los controles de seguridad. Se deberían incluir chequeos de validación en las aplicaciones para la detección de una posible corrupción en la información debida a errores de procesamiento o de acciones	Mediante el establecimiento de una política se debe garantizar que la seguridad es parte integral de los sistemas de información, para evitar errores, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones.

RIESGOS	OBJETIVOS DE CONTROL	CONTROLES	DEFINICIÓN DEL CONTROL
	12 2 Seguridad de las aplicaciones del sistema	deliberadas.	
INFORMACIÓN Documentos			
Robo.	09. Seguridad Física y del Entorno 9 1 Áreas seguras 9.1.3. Seguridad de oficinas, despachos y recursos	Se debería asignar y aplicar la seguridad física para oficinas, despachos y recursos.	Mediante el establecimiento de una política se debe evitar el acceso físico no autorizado, la generación de daños o la realización de intromisiones en las instalaciones y a la información de la organización.
INFORMACIÓN Información Digital			
Corte del suministro eléctrico.	09. Seguridad Física y del Entorno 9 1 Áreas seguras 9.1.4. Protección contra amenazas externas y del entorno	Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	Mediante el establecimiento de una política se debe evitar el acceso físico no autorizado, la generación de daños o la realización de intromisiones en las instalaciones y a la información de la organización.
Errores mantenimiento y actualización de Software. Errores de mantenimiento y actualización de Hardware.	12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información. 12 1 Requisitos de seguridad de los sistemas. 12.1.1. Análisis y especificación de los requisitos de seguridad. 12 2 Seguridad de las aplicaciones del sistema	Las demandas de nuevos sistemas de información para el negocio o mejoras de los sistemas ya existentes deberían especificar los requisitos de los controles de seguridad. Se deberían incluir chequeos de validación en las aplicaciones para la detección de una posible corrupción en la información debida a errores de procesamiento o de acciones deliberadas.	Mediante el establecimiento de una política se debe garantizar que la seguridad es parte integral de los sistemas de información, para evitar errores, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones.

RIESGOS	OBJETIVOS DE CONTROL	CONTROLES	DEFINICIÓN DEL CONTROL
Modificación de la información. Divulgación de información Manipulación de programas Robo	06. Organización de la Seguridad de Información 6 1 Organización Interna 6.1.1. Compromiso de la Dirección con la Seguridad de la Información 6.1.2. Coordinación de la Seguridad de la Información .1.3. Asignación de responsabilidades 6.1.4. Proceso de Autorización de Recursos para el Tratamiento de la Información 6.1.5. Acuerdos de Confidencialidad 6.1.6. Contacto con las Autoridades 6.1.7. Contacto con Grupos de Interés Especial 6.1.8. Revisión Independiente de la Seguridad de la Información	Los miembros de la Dirección deberían respaldar activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la Organización. Las actividades para la seguridad de la información deberían ser coordinadas por representantes que posean de cierta relevancia en su puesto y funciones y de los distintos sectores que forman la Organización. Se deberían definir claramente todas las responsabilidades para la seguridad de la información. Se debería definir y establecer un proceso de gestión de autorizaciones para los nuevos recursos de tratamiento de la información. Se deberían identificar y revisar regularmente en los acuerdos aquellos requisitos de confidencialidad o no divulgación que contemplan las necesidades de protección de la información de la Organización.	Con la labor de un comité para el SGSI se debe gestionar la seguridad de la información dentro de la Organización.

RIESGOS	OBJETIVOS DE CONTROL	CONTROLES	DEFINICIÓN DEL CONTROL
		Se deberían mantener los contactos apropiados con las autoridades pertinentes. Se debería mantener el contacto con grupos o foros de seguridad especializados y asociaciones profesionales. Se deberían revisar las prácticas de la Organización para la gestión de la seguridad de la información y su implantación (por ej., objetivos de control, políticas, procesos y procedimientos de seguridad) de forma independiente y a intervalos planificados o cuando se produzcan cambios significativos para la seguridad de la información.	

RIESGOS	OBJETIVOS DE CONTROL	CONTROLES	DEFINICIÓN DEL CONTROL
PERSONAL			
Errores de los usuarios Suplantación de la identidad del usuario Ingeniería social Extorsión Ingeniería social Extorsión Indisponibilidad del personal	08. Seguridad ligada a los Recursos Humanos 8 1 Seguridad en la definición del trabajo y los recursos 8.1.1. Inclusión de la seguridad en las responsabilidades laborales 8.1.2. Selección y política de personal 8.1.3. Términos y condiciones de la relación laboral	Se deberían definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización. Se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo, contratistas y terceros y en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos. Como parte de su obligación contractual, empleados, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.	Asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.

Fuente: el autor

11. POLÍTICAS DE SEGURIDAD

El establecimiento de las políticas y procedimientos de seguridad requeridos en una organización o empresa es parte de la construcción de un SGSI y se hace con el fin de lograr llevar al mínimo el nivel de riesgo al que pueden estar expuestos los activos informáticos.

En el anexo C de este documento se encuentra la política de seguridad definida para la empresa USOMET Ltda.

12. DIVULGACIÓN

La divulgación de las medidas de seguridad derivadas de este proyecto será gestionada directamente por la gerencia de la empresa USOMET en cuanto haya sido aprobado.

Como medio de divulgación, la gerencia de USOMET ha considerado realizar reuniones de capacitación acompañadas de talleres de refuerzo para todo el personal de la empresa.

13. RESULTADO E IMPACTO

13.1 RESULTADOS

Como resultado del desarrollo de este proyecto se entrega el documento con su contenido completa a la Gerencia de USOMET, convirtiéndose en la base de construcción de su SGSI. Con él pueden realizar la aplicación de las recomendaciones, controles y política de seguridad generados a partir de la identificación de la realidad de la gestión de sus activos informáticos, conforme los requerimientos en la norma ISO/IEC 27001:2013, los objetivos de control de la norma ISO 27002:2013 y la metodología MAGERIT.

Como parte de los resultados se pueden destacar:

- Identificación y Valoración de activos.
- Inventario de activos y procesos.
- Documentación de medidas de seguridad existentes.
- Valoración de vulnerabilidades, amenazas y riesgos.
- Generación de recomendaciones para el tratamiento de riesgos.
- Objetivos de control.
- Política de seguridad.

13.2 IMPACTO

Se han mejorado las relaciones con terceros, clientes y proveedores al lograr hacer más eficientes los procesos en su sistema informático y brindar mayor respaldo a la información.

Se incrementó el nivel de seguridad física de acceso a los dispositivos hardware de todo el sistema, lo que conlleva aumento en la seguridad y reducción de eventos de acceso físico no autorizado.

Se elevó la seguridad del componente lógico de todo el sistema con un mejor manejo del sistema de claves de usuario, más exigente en su creación, cambio periódico, uso y reserva.

14. CONCLUSIONES

Las principales conclusiones obtenidas en esta investigación son:

• Con la elevación de nivel de las medidas de seguridad en el sistema de información se incrementó el respaldo en el manejo de la información y de esa forma la competitividad de la empresa.

• Por primera vez se realizó un estudio detallado de la infraestructura informática y de seguridad en Usomet identificando las condiciones vigentes.

• Se realizó el levantamiento sobre el manejo de la información logrando evaluar e identificar las vulnerabilidades, amenazas y riesgos en sus activos informáticos.

• Se definieron los procedimientos que permiten gestionar la seguridad informática y los mecanismos para la solución de problemas.

• Se elaboró un manual con las políticas aplicables para la gestión de la seguridad del sistema de información.

REFERENCIAS BIBLIOGRÁFICAS

BISOGNO, M. V. (s.f.). Metodología para el aseguramiento de entornos informatizados. Universidad de Buenos Aires. Buenos Aires – Argentina: MAEI. Universidad de Buenos Aires. Obtenido de 2004.

El portal de ISO 27001 en español. (s.f.). Obtenido de ISO 27000.es: http://www.iso27000.es/iso27000.html

ESPAÑA, G. D. (s.f.). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas. Obtenido de protejete.wordpress.com: https://protejete.wordpress.com/

GARCÍA, A. G. (s.f.). Diseño de un sistema de gestión de la seguridad informática SGSI, para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C. a través de la auditoría. Obtenido de unad.edu.co: repository.unad.edu.co/bitstream/10596/3448/1/1030548291.pdf

GUINDEL SÁNCHEZ, E. (2009). Calidad y Seguridad de la información y auditoría informática. Obtenido de http://earchivo.uc3m.es/bitstream/handle/10016/8510/proyectoEsmeralda.pdf;jsessionid=10850A53006DB846CED4EDCEDEDE1C40?sequence=1

GUZMÁN, A., & TABORDA, C. (Abril de 2015). Diseño de un sistema de gestión de la seguridad informática SGSI, para empresas del área textil en las ciudades. Obtenido de UNAD: repository.unad.edu.co/bitstream/10596/3448/1/1030548291.pdf

ISO/IEC. (2013). ISO/IEC 27001 - Information security management. Obtenido de http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

ISO27000.es. (s.f.). Consejos de implantación y métricas de ISO/IEC 27001 y 27002. 2007. Obtenido de ISO27000.es: http://www.iso27000.es/download/ISO_27000_implementation_guidance_v1_Spanish.pdf

JARAMILLO, O. (2008). Estudio de los procesos de seguridad de la información. Obtenido de http://repositorio.utp.edu.co/dspace/bitstream/11059/2370/1/0058S572.pdf

JIMÉNEZ SÁNCHEZ, S. d., LAÍNEZ DURÁN, R., & QUINTANILLA, W. C. (2009). La auditoría interna como una herramienta para establecer controles internos eficientes en las pequeñas y medianas empresas ferreteras de la Ciudad de San Miguel. San Miguel: San Miguel.

UNAD. (s.f.). Riesgos y control informático. Obtenido de http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_1_conceptos_de_vulnerabilidad_riesgo_y_amenaza.html

ANEXOS

Licencia No. 1164 Secretaría de Salud del Dpto. del Tolima
Registro No. 0050027 Cámara de Comercio de Ibagué
NIT 0800092858 - 8
Calle 40 No. 4B-47 Macarena parte alta Ibagué_Tolima
Tels.: 2704500 TeleFax.: 2704501

ANEXO A: POLÍTICA DE SEGURIDAD

USOMET Ltda.

Ibagué, mayo 6 de 2016

INFORMACIÓN DEL DOCUMENTO

TÍTULO	**ANEXO C: POLÍTICA DE SEGURIDAD**
FECHA (aaaa-mm-dd)	2016-05-06
SUMARIO	En este documento se presenta la política de seguridad informática a ser adoptada por la empresa.
PALABRAS CLAVES	Política de seguridad, vulnerabilidad, amenaza, riesgo, control.
VERSIÓN	Versión: 1.0
CATEGORÍA	Documento técnico
AUTOR	Ing. Jaime Hernando Henao Rodríguez
APROBÓ	Gerencia USOMET

CONTROL DE CAMBIOS

VERSIÓN	FECHA	RESPONSABLE	DESCRIPCIÓN
1.0.0	06/05/2016	Gerencia	Establecimiento políticas de seguridad.

TABLA DE CONTENIDO

Pág.

AUDIENCIA

Todo el personal de la empresa USOMET Ltda y las personal que a cualquier título tengan acceso al sistema de información de la empresa. Igualmente aplica a quienes se les solicita adoptar este modelo de seguridad de la información.

POLÍTICA DE SEGURIDAD DEL SGSI

La política de seguridad dentro del Sistema de Gestión de Seguridad de la Información (SGSI) es el documento por el cual establece la posición de la gerencia para indicar: quién, cuándo, por qué, cómo y que, del deber ser del comportamiento para la implementación de medidas sobre el uso del sistema de información (hardware, software e información) de la empresa.

Este documento será actualizado anualmente o por excepción en los siguientes casos:

- Luego de graves incidentes de seguridad
- Luego de una auditoría sin éxito.
- Frente a cambios de la estructura de la organización.

OBJETIVO

Proveer los medios necesarios para alcanzar el aseguramiento de sistema de información.

OBJETIVOS ESPECÍFICOS

Son objetivos de esta política:

- Minimizar los riesgos a los que pueden estar expuestos los activos informáticos de la empresa.
- Aplicar apropiadamente los principios de seguridad de la información.
- Respaldar la confianza en el manejo de información por de las ARL's, los clientes y empleados.
- Continuar el proceso de implementación del sistema de gestión de seguridad de la información.
- Generar una cultura de seguridad de la información en empleados y terceros vinculados a la empresa.

ALCANCE Y APLICABILIDAD

Esta política aplica para todo el personal de la empresa sin distinción ninguna. Los terceros que de alguna forma lleguen a tener acceso al sistema de información también deben refrendar su conocimiento y aceptación mediante la firma de acuerdo individual de conformidad.

NIVEL DE CUMPLIMIENTO

Todo el personal señalado en el alcance y aplicabilidad debe suscribirse al 100% de esta política.

POLÍTICAS

A continuación, se enuncian las políticas de seguridad informática de USOMET Ltda.

POLÍTICA DE ORGANIZACIÓN INTERNA.

Objetivo:
Es decisión de la empresa: definir, implementar evaluar y mejorar en forma permanente un Sistema de Gestión de Seguridad de la Información (SGSI) conforme las necesidades de la empresa y las regulaciones vigentes.

Política:
Para el logro de este objetivo la gerencia conforma este mes el comité responsable del Sistema de Gestión de Seguridad de la Información conformado por la gerencia, subgerencia y coordinadores de área.

POLÍTICA DE RESPONSABILIDAD SOBRE LOS ACTIVOS.

Objetivo:
Definir quién es el responsable que cada activo de información se proteja con la debida seguridad establecida.

Política:
En todo lo relacionado con la seguridad de los activos de la información, el comité de gestión asignará puntualmente en el transcurso del mes de junio 2016, las responsabilidades de cada empleado como propietario del activo. Esta asignación de responsabilidad será comunicada y aceptada por escrito. Además, deberá ser socializada entre empleados y terceros vinculados a la empresa.

POLÍTICA DE SEGURIDAD DIRIGIDA AL RECURSO HUMANO.

Objetivo:
Asegurar que todo el personal vinculado con el sistema de información conozca claramente sus responsabilidades frente a la seguridad y apliquen las normas a fin de reducir los riesgos inherentes.

Política:
La empresa protegerá su sistema de información de las amenazas con origen en el personal de planta o de terceros vinculados mediante la firma de acuerdo de confidencialidad. Formato que será desarrollado y aprobado por el comité de gestión y que debe conocer, aceptar y firmar todo el personal vinculado. Acción que ha de realizarse en el transcurso del mes de junio 2016.

POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO.

Objetivo:
Prevenir el acceso de personal no autorizado a las instalaciones en que se encuentra el sistema de información y evitar así cualquier tipo de daño o intromisión.

Política:
El comité responsable del SGSI, determinará y divulgará los niveles de privilegios de acceso para el personal y la forma de realizar el control físico de acceso a todos los espacios en que está distribuido el sistema de información. Esto puede realizarse mediante sistemas tecnológicos como tarjetas de aproximación, sistemas biométricos o con la ubicación de personal de seguridad. Esta labor tiene como plazo máximo el último día hábil del mes de agosto 2016.

POLÍTICA DE SEGURIDAD PARA EL SUMINISTRO ELÉCTRICO.

Objetivo:
Prevenir el corte de suministro eléctrico, caída de la red de datos o de los equipos ups y baterías de respaldo que pudieran llegar a afectar la operación normal de la empresa.

Política:
Mensualmente se verificará el buen estado de las redes eléctricas que suplen el sistema informático y el cableado de red de datos, así como la protección física de los equipos de cómputo y periféricos.

POLÍTICA DE SEGURIDAD PARA PREVENIR ROBO DE LOS EQUIPOS.

Objetivo:
Identificar los activos y conservar registro de la asignación de responsabilidades para su uso y adecuada protección.

Política:
Todo equipo que haga parte del sistema informático de la empresa debe estar registrado en el inventario de equipos, así como las sucesivas asignaciones a cada empleado para su protección contra: daño, hurto o mal uso. También se debe registrar su devolución en buen estado.

POLÍTICA DE SEGURIDAD PARA ROBO DE INFORMACIÓN.

Objetivo:
Prevenir la fuga de información crítica de la operación de la empresa.

Política:
Se restringe el envío de archivos anexos en los correos generados en la empresa, y la conexión de dispositivos de almacenamiento externo tipo: CD, DVD, USB, etc. además se debe emplear software de cifrado en el almacenamiento de datos y los dispositivos de respaldo de información deben permanecer en el lugar seguro asignado y a esos medios solo debe tener acceso el personal autorizado.

POLÍTICA DE SEGURIDAD EN LOS EQUIPOS.

Objetivo:
Reducir al mínimo la posibilidad de afectación de los activos informáticos evitando el acceso no autorizado a los equipos del sistema.

Política:
La empresa realizará la protección de su infraestructura tecnológica, suprimiendo las vulnerabilidades identificadas, supliendo y verificando los sistemas de respaldo de energía y asegurando que los equipos se disponen en ubicaciones con la menor exposición a acceso no autorizado. Para este efecto la gerencia contratará los servicios de personal especializado. Esta labor debe ser realizada a más tardar el último día hábil del mes de agosto 2016.

POLÍTICA DE PROTECCIÓN CONTRA CÓDIGO MALICIOSO.

Objetivo:
Asegurar la información contra lectura, copia, manipulación, alteración, daño o eliminación mediante el uso de software malicioso.

Política:
La empresa realizará la protección de su información mediante el sistema de protección Windows Defender descargando y activando Microsoft Security Essentials en todos los equipos se su sistema puesto que todos tienen sistema operativo Windows 10.

Para la realización de esta labor se contratará el personal técnico necesario y se debe finalizar antes del último día hábil del mes de mayo.

POLÍTICA DE RESPALDO DE INFORMACIÓN.

Objetivo:
Sostener la disponibilidad de la información con el uso de diferentes medios físicos de respaldo.

Política:
La gerencia dispone de inmediato la creación de la responsabilidad de toma de respaldo de información a cargo de cada empleado. Para el efecto se realizará campaña de capacitación que explique su importancia, la periodicidad de

realización, la forma de hacerlo y la forma de verificarlo. También se suplirán los medios técnicos para su realización.

POLÍTICA SOBRE LA MANIPULACIÓN DE PROGRAMAS.

Objetivo:
Evitar que mediante la manipulación de programas informáticos se afecte de alguna forma la información de la empresa o la operación normal de la misma.

Política:
Solo bajo autorización expresa de la gerencia se podrá realizar la modificación de los programas de uso en su sistema informático, de esta forma quien sea autorizado es responsable de los resultados y debe dejar por escrito que el software no contiene rutinas mal intencionadas que pudieran llegar a afectar la información o la normal operación del sistema.

POLÍTICA SOBRE EL MANTENIMIENTO DE HARDWARE Y SOFTWARE.

Objetivo:
Prevenir que la realización del mantenimiento preventivo o correctivo de los componentes del sistema informático de la empresa pudiera ser empleado para afectar de alguna manera los datos o la operación del sistema.

Política:
Solo bajo autorización expresa de la gerencia se podrá realizar el mantenimiento preventivo o correctivo de los programas y equipos de uso en su sistema informático, de esta forma quien sea autorizado es responsable de los resultados y debe dejar constancia por escrito que el software no contiene rutinas mal intencionadas que pudieran llegar a afectar la información o dispositivos físicos defectuosos que limiten la normal operación del sistema.

POLÍTICA SOBRE LA INGENIERÍA SOCIAL.

Objetivo:
Evitar que los empleados de la empresa sean víctimas del delito informático denominado ingeniería social.

Política:
La empresa adelantará periódicamente talleres de concientización sobre los diferentes tipos de delitos informáticos de los que podrían ser víctimas a fin de resguardar la información confidencial de la empresa y de todo lo relacionado al sistema de información, para evitar que sean manipulados por personas que ganando su confianza obtengan información privilegiada.

POLÍTICA SOBRE DESTRUCCIÓN DE INFORMACIÓN.

Objetivo:
Reducir al máximo la posibilidad de pérdida parcial o total de información administrada en el sistema informático de la empresa.

Política:
La toma de copias de seguridad de la información con los ciclos establecidos (diarios, semanales, mensuales) es de obligatorio cumplimiento para todos los responsables de su realización. Los medios de almacenamiento empleados deberán ser conservados exclusivamente en los sitios seguros asignados al efecto.

POLÍTICA SOBRE ABUSO DE PRIVILEGIOS DE ACCESO.

Objetivo:
Evitar el ataque deliberado al sistema realizado mediante el abuso de privilegios de acceso asignados a los empleados de la empresa o a terceros relacionados.

Política:
Todos los sistemas informáticos de uso en la empresa deben registrar las acciones de los usuarios llevando bitácora a la que no deben tener acceso ellos mismos.

POLÍTICA DE SEGURIDAD DE LAS REDES.

Objetivo:
Brindar seguridad a la información que circula en la red de la empresa y cuando esta se conecta a redes externas.

Política:
La gerencia ordenará la verificación periódica de la red de la empresa para garantizar: su seguridad, su estabilidad, la certificación del cableado y dispositivos de red y vigencia del diseño lógico y físico, esta labor se realizará semestralmente a partir del primer día hábil del mes de junio.

POLÍTICA DE INTERCAMBIO DE INFORMACIÓN Y SOFTWARE.

Objetivo:
Evitar la exposición a lectura, copia, manipulación, alteración, daño o eliminación no autorizada de información de la empresa cuando se lleva a cabo el intercambio de información o de software.

Política:
La empresa protegerá mediante controles técnicos como: inhabilitación de puertos USB, inhabilitación para el envío de archivos anexos en los correos de los

empleados, de tal forma que solo bajo autorización expresa se puedan realizar estas acciones con la información que se transmite como parte de los procesos propios del negocio, a fin de reducir el impacto de cualquier orden que pudiera afectar el normal desarrollo de las actividades de la empresa. El comité de gestión revisará trimensualmente a partir de este mes la vigencia del ciclo de vida de las aplicaciones software adquiridas o desarrolladas en la empresa a fin de garantizar su vigencia y actualización.

POLÍTICA PARA LA GESTIÓN DE INCIDENTES.

Objetivo:
Asegurar que las vulnerabilidades de los activos en el sistema de información sean reconocidas oportunamente y se establezcan y den a conocer los correctivos a aplicar oportunamente.

Política:
El comité de gestión puede desarrollar o contratar el desarrollo de planes de continuidad y contingencia de forma que se cuente con la identificación de las acciones apropiadas para el manejo de la mayor cantidad de eventos previsible de todo orden que pudieran llegar a afectar cualquiera de los activos de información de manera alguna.

SANCIONES.

El comité responsable del SGSI, determinará la sanción a aplicar en cada caso de incumplimiento de cualquiera de las políticas aquí indicadas teniendo en cuenta:

- La gravedad del incumplimiento.
- El daño o afectación al activo de información relacionado con el caso.
- La reiteración de incumplimientos de las políticas de seguridad, elevará gradualmente la sanción a aplicar.

Entre las sanciones pueden estar:

- Reconvención verbal sin anotación a la hoja de vida.
- Reconvención verbal con anotación a la hoja de vida.
- Suspensión por un día en el cargo.
- Despido justificado por incumplimiento reiterativo de las políticas de seguridad.

Ibagué, 6 mayo de 2016.

ORIGINAL FIRMADO POR LA GERENTE DE USOMET Ltda.

ANEXO B

PROCEDIMIENTOS DOCUMENTADOS.

USOMET LTDA.

TABLA DE CONTENIDO

Pág.

1. PROCEDIMIENTOS DOCUMENTADOS

Un proceso es la realización de una actividad mediante un método. Para facilitar su aplicación en forma correcta se hace necesario que se documente, donde de manera breve pero clara y sencilla se den las indicaciones de los pasos a realizar conforme el método adoptado.

En USOMET se cuenta con los siguientes procedimientos:

1. Procedimiento para copias de seguridad
2. Procedimiento para actualización de software
3. Procedimiento para cambio de software
4. Procedimiento para cambio de hardware
5. Procedimiento para registro de usuarios en el sistema de servicio de la empresa
6. Procedimiento para retiro de usuarios en el sistema de servicio de la empresa
7. Procedimiento para Levantamiento de panorama de riesgos
8. Procedimiento para Capacitación en gestión de riesgos industriales
9. Procedimiento para Evaluación de salud ocupacional
10. Procedimiento para Gestión documental física, correspondencia física, trámites empresariales

1.1 PROCEDIMIENTO PARA COPIAS DE SEGURIDAD.

Este procedimiento describe el método para realizar las copias de seguridad de la información digital de la empresa.

1.1.1 OBJETIVO: Brindar respaldo al principal activo informático de la empresa, la información, guardando a diario copia en un lugar con las apropiadas condiciones de seguridad.

1.1.2 ALCANCE: Obtener respaldo permanente de toda la información atinente a la gestión de la empresa.

1.1.3 DEFINICIONES:

Base de datos: Forma de almacenar y consultar información en un formato específico que facilita su organización, mantenimiento y consulta hasta grandes volúmenes de datos.

Disco duro: Disco metálico con un sustrato magnético en la capa superior. Se puede hacer analogía con los discos de música, en su forma de funcionar,

permiten almacenar, consultar, modificar y eliminar información en grandes volúmenes de datos.

Esquema de rotación de backup: La realización de copias de seguridad (backup) es un método que permite dar respaldo eficaz a la información digital. Existen múltiples modelos de organización de toma de Backups, entre otros se aconseja diferentes copias tomadas con los menores espacios de tiempo posibles entre unos y otros.

Sitio de backup: Se aconseja disponer de un sitio alterno para la conservación y puesta en funcionamiento el sistema a partir de las copias de seguridad, utilizable en casos de inconvenientes de uso en el sitio principal.

Ventana de backup: Son los espacios de tiempo en los que se procede a la toma de los Backups. Siempre teniendo en cuenta los volúmenes de información a respaldar y la intensidad de transacciones que pudieran ser ralentizadas a causa del proceso.

Cronología copias de seguridad: El respaldo de los archivos seleccionados requiere la definición de una cronología para su adecuada realización, por lo cual se sugiere el siguiente esquema:

copia de seguridad total anual
copia de seguridad total mensual
copia de seguridad total diaria de archivos
copia de seguridad diferencial diaria para la base de datos

Recuperación/recuperación de datos: El respaldo de información no solo consiste en la toma de backup, sino en la prueba periódica de la plena funcionalidad de la información respaldada mediante su recuperación de ser posible en equipos alternos.

Copia de seguridad diferencial: Una alternativa a la copia de seguridad plena permanente consiste en hacer un respaldo total en períodos largos y unos backup de la nueva información en períodos más cortos, agilizando de esta forma todo el proceso.

Recuperación ante desastres: Como uno de los pilares de los planes de contingencia y recuperación está el de cómo se debe realizar la recuperación de un sistema ante eventuales desastres por lo cual se debe planear anticipadamente las acciones que deban realizarse si se presenta el caso específico.

1.1.4 CONDICIONES GENERALES: Bajo ninguna circunstancia debe dejarse de realizar este procedimiento por parte del responsable de mimo o por quien haga sus veces en su ausencia, por lo cual también debe conocer cabalmente este procedimiento.

1.1.5 DESCRIPCIÓN DEL PROCEDIMIENTO: El procedimiento de copia de seguridad se base en el respaldo necesario para los datos de la gestión de la empresa.

Tabla 1: Procedimiento de Gestión de copias de seguridad.

N	ACTIVIDAD	RESPONSABLE	REGISTRO
1	Verificar disponibilidad de los medios físicos de respaldo y solicitar con debida anticipación se suplan los elementos necesarios.	Amparo Sánchez	Bitácora de copias de seguridad.
2	Realizar la copia o copias de seguridad correspondientes de los archivos a la fecha, en el rango Horario dispuesto para el efecto.	Amparo Sánchez	Bitácora de copias de seguridad.
3	Realizar la copia o copias de seguridad correspondientes de la base de datos a la fecha, en el rango Horario dispuesto para el efecto.	Amparo Sánchez	Bitácora de copias de seguridad.
4	Depositar los medios de copia de seguridad en los espacios seguros asignados.	Amparo Sánchez	Bitácora de copias de seguridad.
5	Periódicamente se debe realizar la verificación de la calidad de registro en los medios de respaldo.	Amparo Sánchez	Bitácora de copias de seguridad.

Fuente: El autor.

1.1.6 RESPONSABLES: **Amparo Sánchez**

1.1.7 DURACIÓN DEL PROCEDIMIENTO: El tiempo total empleado en este proceso es de alrededor de 30 minutos.

1.2 PROCEDIMIENTO PARA ACTUALIZACIÓN DE SOFTWARE

Este procedimiento describe el método para actualización de software de la empresa.

1.2.1 OBJETIVO: Asegurar que la actualización de software se realice en forma autorizada, previa verificación de calidad de la nueva versión.

1.2.2 ALCANCE: Mantener actualizado él software de la empresa para que se aprovechen las últimas mejoras en funcionalidad y corrección de errores.

1.2.3 DEFINICIONES:

Actualización de un programa: Proceso con el que se mantiene la vigencia del software ante los cambios de operación para el cual fue diseñado y a su vez la corrección de errores detectados en versiones anteriores.

Software: Es el conjunto de instrucciones que mediante la programación desde cualquier lenguaje de programación hace que el hardware efectué determinadas acciones digitales o físicas (ejemplo las impresoras).

1.2.4 CONDICIONES GENERALES: Cuando se tenga conocimiento de la disponibilidad de una nueva versión del software se procederá a indagar sus bondades y a determinar su adquisición.

1.2.5 DESCRIPCIÓN DEL PROCEDIMIENTO: El procedimiento de actualización de software se realiza cada vez que se tiene conocimiento de que una nueva versión está disponible.

Tabla 2: Procedimiento para la actualización de software.

N	ACTIVIDAD	RESPONSABLE	REGISTRO
1	Verificación con el proveedor de nueva versión disponible.	Amparo Sánchez	Bitácora de actualización de software.
2	Realización de pruebas de calidad de la nueva versión.	Amparo Sánchez	Bitácora de actualización de software.
3	Aprobación de pruebas de calidad de la nueva versión y costos.	Amparo Sánchez	Bitácora de actualización de software.
4	Planeación del cronograma de actualización por equipos.	Amparo Sánchez	Bitácora de actualización de software.
5	Realización de la actualización equipo por equipo.	Amparo Sánchez	Bitácora de actualización de software.
6	Capacitación de usuarios sobre cambios en el software.	Proveedor del software	Bitácora de actualización de software.

Fuente: El autor.

1.2.6 RESPONSABLES: Amparo Sánchez, proveedor del software.

1.2.7 DURACIÓN DEL PROCEDIMIENTO: Todo el proceso de actualización de software y capacitación no debe tomar más de cinco días hábiles.

1.3 PROCEDIMIENTO PARA CAMBIO DE SOFTWARE

Este procedimiento describe el método para determinar y realizar el cambio de software.

1.3.1 OBJETIVO: Asegurar que la empresa cuente con las mejores herramientas informáticas para su gestión.

1.3.2 ALCANCE: Sin estar haciendo erogaciones innecesarias, mantener al día el software de gestión que le sea de mayor utilidad a la empresa.

1.3.3 DEFINICIONES:

Software: Es el conjunto de instrucciones que mediante la programación desde cualquier lenguaje de programación hace que el hardware efectué determinadas acciones digitales o físicas (ejemplo las impresoras).

1.3.4 CONDICIONES GENERALES: Cuando se tenga conocimiento de la disponibilidad de un software que mejore la gestión de información en la empresa se procederá a indagar sus bondades y a determinar su adquisición.

1.3.5 DESCRIPCIÓN DEL PROCEDIMIENTO: El procedimiento para la adquisición de software se realiza cada vez que se tiene conocimiento de la disponibilidad de un buen producto y se procede así:

Tabla 3: Procedimiento para la adquisición de software.

N	ACTIVIDAD	RESPONSABLE	REGISTRO
1	Verificación con el proveedor de sobre por qué su software tendría un valor agregado para la gestión de la empresa.	Amparo Sánchez	Bitácora de adquisición de software.
2	Realización de pruebas de características del producto.	Amparo Sánchez	Bitácora de adquisición de software.
3	Aprobación de pruebas y costos.	Amparo Sánchez	Bitácora de adquisición de software.
4	Planeación del cronograma de implantación por equipos.	Amparo Sánchez	Bitácora de adquisición de software.
5	Realización de la implantación equipo por equipo.	Amparo Sánchez	Bitácora de adquisición de software.
6	Capacitación de usuarios sobre el nuevo software.	Proveedor del software	Bitácora de adquisición de software.

Fuente: El autor.

1.3.6 RESPONSABLES: Amparo Sánchez, proveedor del software.

1.3.7 DURACIÓN DEL PROCEDIMIENTO: El tiempo del proceso de adquisición e implementación de software y capacitación depende del producto a ser comprado y sus dimensiones funcionales.

1.4 PROCEDIMIENTO PARA CAMBIO DE HARDWARE

Este procedimiento describe el método para determinar cuándo realizar el cambio de hardware.

1.4.1 OBJETIVO: Mantener vigente la plataforma hardware de la empresa acorde con la tecnología de vanguardia que ofrezca mejoras significativas en capacidad de cómputo.

1.4.2 ALCANCE: Sin incurrir en gastos innecesarios, disponer del hardware de apoyo a la gestión de la empresa, que cuente con las mejores características técnicas.

1.4.3 DEFINICIONES:

Hardware: Parte física del sistema informático principalmente computadores y periféricos, con todos sus componentes internos que determinan su poder de computo.

1.4.4 CONDICIONES GENERALES: Conforme el volumen de información de la empresa crece, la demanda de realización de procesos con esa información, mayor volumen mayor velocidad, la necesidad de contar con comunicaciones más ágiles, etc. Conllevan la necesidad de contar con mayor poder de cómputo, lo cual se evidencia alrededor de cada dos años, lo cual obliga a la renovación paulatina de equipos.

1.4.5 DESCRIPCIÓN DEL PROCEDIMIENTO: El procedimiento para la adquisición de hardware se realiza periódicamente y se procede de la siguiente forma:

Tabla 4: Procedimiento para la adquisición de hardware.

N	ACTIVIDAD	RESPONSABLE	REGISTRO
1	Verificación de las condiciones de los equipos actuales en la empresa, de la necesidad de incrementar la capacidad de cómputo y de renovación de equipos.	Amparo Sánchez	Actas de adquisición de Equipos.
2	Realización de determinación de requerimientos y cotizaciones.	Amparo Sánchez	Actas de adquisición de Equipos.
3	Aprobación de identificación de requerimientos cotizaciones y costos.	Amparo Sánchez	Actas de adquisición de Equipos.
4	Planeación del cronograma de adquisición e instalación de equipos y toma de respaldo de la información uno a uno.	Amparo Sánchez	Actas de adquisición de Equipos.
5	Realización del cambio de equipo uno a uno haciendo la restauración de información.	Amparo Sánchez	Actas de adquisición de Equipos.

Fuente: El autor.

1.4.6 RESPONSABLES: Amparo Sánchez, proveedor del hardware.

1.4.7 DURACIÓN DEL PROCEDIMIENTO: El tiempo del proceso de adquisición e instalación de hardware depende del producto a ser comprado y disponibilidad del proveedor.

1.5 PROCEDIMIENTO PARA REGISTRO DE USUARIOS EN EL SISTEMA DE SERVICIO DE LA EMPRESA

Este procedimiento describe el método para solicitar y registrar usuarios en el sistema de la empresa.

1.5.1 OBJETIVO: Realizar de manera formal el control de registro de usuarios en el sistema.

1.5.2 ALCANCE: Todo el personal vinculado a la empresa que deba acceder al sistema solo podrá hacerlo con su propia cuenta y clave.

1.5.3 DEFINICIONES:

Usuario de sistema: Característica que se otorga a una persona cuando se registra en un sistema informático quedando caracterizado con un perfil que le habilita a realizar determinadas acciones dentro del sistema.

1.5.4 CONDICIONES GENERALES: El sistema es el corazón del manejo de información de la gestión de la empresa, su manejo debe ser cuidadoso y solo las personas autorizadas deben tener acceso a las funcionalidades del sistema para lo cual deben contar con un registro de usuario.

1.5.5 DESCRIPCIÓN DEL PROCEDIMIENTO: El procedimiento para el registro de una persona como usuario del sistema se realiza de la siguiente forma:

Tabla 5: Procedimiento para el registro de usuarios.

N	ACTIVIDAD	RESPONSABLE	REGISTRO
1	En el mismo sistema se llena un formato de solicitud por parte del peticionario.	Cada usuario	Registro de usuarios del sistema.
2	El administrador del sistema aprueba la solicitud asignando el perfil requerido.	Amparo Sánchez	Registro de usuarios del sistema.
3	Al correo del peticionario le llega un mensaje informando la aprobación del registro de usuario.	Amparo Sánchez	Registro de usuarios del sistema.
4	El nuevo usuario puede acceder al sistema hacer uso de las funciones asignadas a su perfil.	Amparo Sánchez	Registro de usuarios del sistema.
	El nuevo usuario recibe una capacitación expedita en el	Amparo Sánchez	Registro de usuarios del

5	uso de las características del sistema asignadas a su perfil.		sistema.

Fuente: El autor.

1.5.6 RESPONSABLES: Nuevo usuario, Amparo Sánchez.

1.5.7 DURACIÓN DEL PROCEDIMIENTO: El tiempo del proceso de registro y aprobación de usuario puede ser de unos cinco minutos, el tiempo de capacitación depende de las funcionalidades del sistema asignadas a su perfil.

1.6 PROCEDIMIENTO PARA RETIRO DE USUARIOS EN EL SISTEMA DE SERVICIO DE LA EMPRESA

Este procedimiento describe el método para solicitar el registro de un usuario en el sistema de la empresa.

1.6.1 OBJETIVO: Realizar de manera formal el control de registro de usuarios en el sistema.

1.6.2 ALCANCE: Todo el personal vinculado a la empresa que haya sido registrado como usuario del sistema y ya no deba tener esa condición debe ser caracterizado como inactivo, suspendiendo toda posibilidad de acceso.

1.6.3 DEFINICIONES:

Usuario de sistema: Característica que se otorga a una persona cuando se registra en un sistema informático quedando caracterizado con un perfil que le habilita a realizar determinadas acciones dentro del sistema.

Usuario inactivo: Característica que se otorga a una persona cuando ha estado registrada en el sistema informático quedando caracterizado como que en algún momento fue parte de los usuarios del sistema y allí quedaron registradas sus acciones pero que ya no cuenta más con los privilegios otorgados.

1.6.4 CONDICIONES GENERALES: El sistema es el corazón del manejo de información de la gestión de la empresa, su manejo debe ser cuidadoso y solo las personas autorizadas deben tener acceso a las funcionalidades del sistema para lo cual se debe catalogar como inactivo a un usuario que ya no deba tener acceso.

1.6.5 DESCRIPCIÓN DEL PROCEDIMIENTO: El procedimiento para calificar como inactivo el registro de una persona como usuario del sistema se realiza de la siguiente forma:

Tabla 6: Procedimiento para el registro de usuarios.

N	ACTIVIDAD	RESPONSABLE	REGISTRO
1	En jefe inmediato registra en el sistema la calificación de inactivo al usuario que ahora deba tener esa condición.	Jefe inmediato del usuario	Registro de usuarios del sistema.

Fuente: El autor.

1.6.6 RESPONSABLES: Jefe inmediato del usuario.

1.6.7 DURACIÓN DEL PROCEDIMIENTO: El tiempo del proceso de cambio de estado del registro de usuario está alrededor de cinco minutos.

1.7 PROCEDIMIENTO PARA LEVANTAMIENTO DE PANORAMA DE RIESGOS

Este procedimiento describe el método para realizar el levantamiento de panorama de riesgos.

1.7.1 OBJETIVO: Realizar el levantamiento de panoramas de riesgo que son contratados por las empresas en el Tolima para la gestión de la seguridad industrial y salud ocupacional.

1.7.2 ALCANCE: Toda actividad empresarial requiere una evaluación periódica del panorama de riesgos conforme el desarrollo de sus actividades en cada etapa de proceso. USOMET realiza esta labor por lo cual es contratada durante todo el año.

1.7.3 DEFINICIONES:

Panorama de riesgos: Documento detallado en el que se identifican los riesgos a los que están expuestos los equipos de trabajo en las diferentes áreas de las empresas y que pueden tener implicaciones en la salud ocupacional de los empleados y en su productividad.

1.7.4 CONDICIONES GENERALES: En razón a que la contratación para el levantamiento de panorama de riesgos puede aumentar o decrecer en el transcurso de cada mes, la empresa tiene un responsable del tema, pero contrata los profesionales necesarios en el momento requerido por el sistema de prestación de servicios.

1.7.5 DESCRIPCIÓN DEL PROCEDIMIENTO: El procedimiento para el levantamiento del panorama de riesgos se realiza de la siguiente forma:

Tabla 7: Procedimiento para la realización en el levantamiento de panorama de riesgos.

N	ACTIVIDAD	RESPONSABLE	REGISTRO
1	Un cliente contrata la empresa para que se le realice el levantamiento del panorama de riesgos y se establece un cronograma de trabajo.	Cliente y Gerente de la empresa	Contrato.
2	USOMET realiza la planeación y se definen: metas, responsables, indicadores de gestión, períodos para hacer, momentos para verificar y períodos para actuar. Para cada contrato y se contrata el personal requerido según el caso.	Gerente y subgerente	Documento de ejecución para cada contrato
3	El personal contratado realiza el levantamiento en sitio del panorama de riesgos conforme los estándares determinados por la empresa, registrando los resultados en el sistema de servicios.	Personal contratado	Documento de ejecución para cada contrato
4	El jefe del área aprueba o solicita la realización de ajustes al informe presentado.	Personal contratado	Documento de ejecución para cada contrato
5	Aprobado el informe se le entrega a la empresa contratante.	Jefe del área	Documento de ejecución para cada contrato

Fuente: El autor.

1.7.6 RESPONSABLES: Gerente, subgerente, jefe de área y personal contratado.

1.7.7 DURACIÓN DEL PROCEDIMIENTO: El levantamiento de panorama de riesgos no tiene un tiempo fijo pues depende de varios factores como son: el tamaño de la empresa contratante, en número de áreas y labores a cubrir y la disponibilidad de personal calificado a contratar.

1.8 PROCEDIMIENTO PARA CAPACITACIÓN EN GESTIÓN DE RIESGOS INDUSTRIALES

Este procedimiento describe el método para realizar Capacitación en gestión de riesgos industriales.

1.8.1 OBJETIVO: Realizar las capacitaciones en gestión de riesgos industriales que son contratados por las empresas en el Tolima para la gestión de la seguridad industrial y salud ocupacional.

1.8.2 ALCANCE: Toda actividad empresarial requiere que su personal cuente con la capacitación apropiada y necesaria para el manejo de los riesgos industriales, USOMET es una empresa especializada en esta labor por lo cual es contratada a lo largo del año.

1.8.3 DEFINICIONES:

Panorama de riesgos: Documento detallado en el que se identifican los riesgos a los que están expuestos los equipos de trabajo en las diferentes áreas de las empresas y que pueden tener implicaciones en la salud ocupacional de los empleados y en su productividad.

1.8.4 CONDICIONES GENERALES: En razón a que la contratación para la capacitación en riesgos industriales puede aumentar o decrecer en el transcurso de cada mes, la empresa tiene un responsable del tema, pero contrata los profesionales necesarios en el momento requerido por el sistema de prestación de servicios.

1.8.5 DESCRIPCIÓN DEL PROCEDIMIENTO: El procedimiento para la realización de capacitación en riesgos industriales se realiza de la siguiente forma:

Tabla 8: Procedimiento para la capacitación en riesgos industriales.

N	ACTIVIDAD	RESPONSABLE	REGISTRO
1	Un cliente contrata la empresa para que se le realice capacitación en riesgos industriales y se establece un cronograma de trabajo.	Cliente y Gerente de la empresa	Contrato.
2	USOMET realiza la planeación y se definen: metas, responsables, indicadores de gestión, períodos para hacer, momentos para verificar y períodos para actuar. Para cada contrato y se contrata el personal requerido según el caso.	Gerente y subgerente	Documento de ejecución para cada contrato, sistema.
3	El personal contratado realiza la capacitación conforme las actividades a cubrir con el contrato.	Personal contratado	Documento de ejecución para cada contrato, sistema.
4	El jefe del área aprueba la realización de la capacitación.	Personal contratado	Documento de ejecución para cada contrato, sistema.

Fuente: El autor.

1.8.6 RESPONSABLES: Gerente, subgerente, jefe de área y personal contratado.

1.8.7 DURACIÓN DEL PROCEDIMIENTO: La capacitación en gestión de riesgos industriales se realiza en un día hábil por área a cubrir dentro de las labores de una empresa.

1.9 PROCEDIMIENTO PARA EVALUACIÓN DE SALUD OCUPACIONAL

Este procedimiento describe el método para realizar la evaluación de salud ocupacional al personal vinculado o a contratar en las empresas contratantes.

1.9.1 OBJETIVO: Realizar y entregar resultados de las evaluaciones médicas estándar al personal que las empresas tiene contratado o va a contratar para su planta de personal.

1.9.2 ALCANCE: Las empresas requieren que el personal a ser contratado o está laborando o se retira del servicio, sea evaluado médicamente en los factores estándar determinados legalmente.

1.9.3 DEFINICIONES:

La Resolución 2346 de 2007: Establece como elemento clave para el diagnóstico de las condiciones de salud de los empleados la realización de evaluaciones médicas ocupacionales, de forma que permitan plantear y ejecutar programas médicos preventivos.

Panorama de riesgos: Documento detallado en el que se identifican los riesgos a los que están expuestos los equipos de trabajo en las diferentes áreas de las empresas y que pueden tener implicaciones en la salud ocupacional de los empleados y en su productividad.

1.9.4 CONDICIONES GENERALES: En razón a que la contratación para la capacitación en riesgos industriales puede aumentar o decrecer en el transcurso de cada mes, la empresa tiene un responsable del tema, pero contrata los profesionales necesarios en el momento requerido por el sistema de prestación de servicios.

1.9.5 DESCRIPCIÓN DEL PROCEDIMIENTO: El procedimiento para la realización de evaluaciones de salud ocupacional se realiza de la siguiente forma:

Tabla 9: Procedimiento para la realización de evaluaciones de salud ocupacional.

N	ACTIVIDAD	RESPONSABLE	REGISTRO
1	Un cliente contrata la empresa para que se le realice capacitación en riesgos industriales y se establece un cronograma de trabajo.	Cliente y Gerente de la empresa	Contrato.
2	USOMET realiza la planeación y se definen: metas, responsables, indicadores de gestión, períodos para hacer, momentos para verificar y períodos para actuar. Para cada contrato y se contrata el personal requerido según el caso.	Gerente y subgerente	Documento de ejecución para cada contrato, sistema.
3	El personal contratado realiza las evaluaciones estándar en salud ocupacional al personal remitido por las empresas, registrando los resultados en el sistema de servicio.	Personal contratado	Documento de ejecución para cada contrato, sistema.
4	El jefe del área aprueba las evaluaciones realizadas y hace los análisis de resultados que posteriormente son remitidos a las empresas contratantes.	Personal contratado	Documento de ejecución para cada contrato, sistema.

Fuente: El autor.

1.9.6 RESPONSABLES: Gerente, subgerente, jefe de área y personal contratado.

1.9.7 DURACIÓN DEL PROCEDIMIENTO: Las evaluaciones estándar en salud ocupacional tardan alrededor de un día hábil.

1.10 PROCEDIMIENTO PARA GESTIÓN DOCUMENTAL FÍSICA, CORRESPONDENCIA FÍSICA, TRÁMITES EMPRESARIALES

Este procedimiento describe el método para la gestión documental física, correspondencia física, trámites empresariales.

1.10.1 OBJETIVO: Mantener al día la gestión documental de la empresa de forma que la documentación este segura, ordenada y disponible todo el tiempo.

1.10.2 ALCANCE: Las empresas requieren que la documentación producto de su gestión sea administrada técnicamente de forma que se tenga la certeza de su seguridad, orden y disponibilidad.

1.10.3 DEFINICIONES:

La gestión documental: Actualmente la mayoría de los sistemas de gestión documental son manejados mediante aplicaciones software con el uso intensivo de bases de datos. Estas aplicaciones han evolucionado enormemente con el aprovechamiento de la tecnología para dar el adecuado tratamiento a documentos de tipo, entre otros: científicos, culturales y técnicos.

1.10.4 CONDICIONES GENERALES: Debido al elevado volumen de documentos que se genera en la contratación de la empresa con sus clientes y en el desarrollo de los contratos, se hace indispensable realizar su gestión mediante sistemas automatizados y bajo los lineamientos estándar de gestión documental.

1.10.5 DESCRIPCIÓN DEL PROCEDIMIENTO: El procedimiento para la realización de evaluaciones de salud ocupacional se realiza de la siguiente forma:

Tabla 10: Procedimiento para la realización de Gestión documental física, correspondencia física, trámites empresariales.

N	ACTIVIDAD	RESPONSABLE	REGISTRO
1	Se produce documentación como parte de la gestión de la empresa.	Amparo Sánchez	Sistema Gestión Documental.
2	Con el uso del Sistema de Gestión documental y las normas estándar de manejo de documentos, se clasifican y registran en el sistema con imagen de cada uno.	Amparo Sánchez	Sistema Gestión Documental.
3	La documentación física se almacena ordenadamente en los estantes señalizados dispuestos para el efecto.	Amparo Sánchez	Sistema Gestión Documental.
4	La información registrada en el sistema y la imagen escaneada están a disposición de cualquiera de los empleados de la empresa registrados en él sistema.	Amparo Sánchez	Sistema Gestión Documental.

Fuente: El autor.

1.10.6 RESPONSABLES: Amparo Sánchez.

1.10.7 DURACIÓN DEL PROCEDIMIENTO: La labor de clasificación, registro en el sistema y disposición de almacenamiento de la documentación es una labor de carácter permanente en la medida que la documentación se genera.

ANEXO C (Solicitud enviada a la gerente de USOMET Ltda.)

Bogotá, 21 de septiembre de 2015

Doctora
ALBA NIDIA SANCHEZ CEDIEL
Gerente
USOMET LTDA.

Apreciada Doctora Alba Nidia:

Como es de su conocimiento actualmente me encuentro terminando la especialización en seguridad informática en la universidad UNAD. Como parte de los requisitos se debe realizar el desarrollo de un proyecto en seguridad informática en una empresa a nuestro alcance.

Esta es una buena oportunidad de aprovechar esta labor para establecer en su empresa un sistema de gestión en seguridad informática con los beneficios que conlleva. Por lo cual solicito su autorización para adelantar la gestión necesaria en el desarrollo proyecto de grado.

De antemano agradezco la atención prestada y quedo atento a su positiva respuesta.

Atentamente,

Jaime Hernando Henao Rodríguez
c.c.19.307.458 de Bogotá

ANEXO D (Respuesta de aprobación de la gerente de USOMET Ltda.)

Licencia No. 1164 Secretaría de Salud del Dpto. del Tolima
Registro No. 0050027 Cámara de Comercio de Ibagué
NIT 0800092858 - 8
Calle 40 No. 4B-47 Macarena parte alta Ibagué_Tolima
Tels.: 2704500 TeleFax.: 2704501

Ibagué, 22 de septiembre de 2015

Señores
Universidad Nacional Abierta y a Distancia – UNAD
Posgrado en Especialización en Seguridad Informática
Ciudad

Cordial saludo:

La gerencia de USOMET identificada con NIT 800092858 ha recibido solicitud del ingeniero JAIME HERNANDO HENAO RODRÍGUEZ, c.c.19.307.458 de Bogotá, quien presta servicios de asesoría en el área informática a esta empresa, para realizar en la misma el desarrollo de un proyecto en seguridad informática, como parte de la culminación de sus estudios de postgrado en esa Institución.

La gerencia acoge la propuesta y la aprueba autorizando su realización con toda la colaboración, disposición y espacio requeridos para llevar a cabo el respectivo proyecto.

Atentamente,

Unidad de Salud Ocupacional
y Medicina del Trabajo
Alba Nidia Sánchez Cediel
Ing. Ind. Salubrologa Ocupacional
Lic.1164 S.S. Gerente

ALBA NIDIA SÁNCHEZ CEDIEL
Gerente

RESUMEN RAE

1.Información General	
Tipo de documento	Tesis de Grado
Acceso al documento	Universidad Nacional Abierta y a Distancia - UNAD
Título del documento	Diseño de un Sistema de Gestión de Seguridad Informática basado en la norma ISO/IEC 27001:2013 para la empresa USOMET Ltda. en la ciudad de Ibagué.
Autores	HENAO, Jaime
Director	GONZÁLEZ, Salomón
Publicación	Bogotá. Universidad Nacional Abierta y a Distancia UNAD, 2016. Páginas: 129.
Unidad Patrocinante	USOMET Ltda. Ibagué, Tolima, Colombia.
Palabras Claves	ISO/IEC 27001:2013, SGSI, Vulnerabilidad, Riesgo, Amenaza, Activos de Información, MAGERIT, Gestión de Riesgo, Control, Políticas de seguridad.

2.Descripción
Este proyecto se desarrolla para comprobar los beneficios al mejorar el nivel de seguridad del sistema informático de la empresa USOMET de la ciudad de Ibagué, Mediante el diseño de un SGSI que permita mitigar las amenazas y vulnerabilidades presentes y gestionar adecuadamente los riesgos en cada uno de los activos de información.

3.Fuentes
Bisogno, M. V. (s.f.). *Metodología para el aseguramiento de entornos informatizados – Universidad de Buenos Aires.* Buenos Aires – Argentina: MAEI. Universidad de Buenos Aires. Obtenido de 2004. *Calidad y Seguridad de la información y auditoría informática*, disponible en internet en: http://earchivo.uc3m.es/bitstream/handle/10016/8510/proyectoEsmeralda.pdf;jsessionid=10850A53006DB846CED4EDCEDEDE1C40?sequence=1 *El portal de ISO 27001* en español. (s.f.). Obtenido de ISO 27000.es: http://www.iso27000.es/iso27000.html España, G. D. (s.f.). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas.* Obtenido de protejete.wordpress.com: https://protejete.wordpress.com/ García, A. G. (s.f.). *Diseño de un sistema de gestión de la seguridad informática SGSI, para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C. a través de la auditoría.* Obtenido de unad.edu.co: repository.unad.edu.co/bitstream/10596/3448/1/1030548291.pdf *Gestión estratégica de seguridad en la empresa*, disponible en internet en:

http://video.anetcom.es/editorial/Seguridad_empresa.pdf

Guzmán, A. T. (Abril de 2015). *Diseño de un sistema de gestión de la seguridad informática SGSI, para empresas del área textil en las ciudades .* Obtenido de UNAD: repository.unad.edu.co/bitstream/10596/3448/1/1030548291.pdf

ISO/IEC. (2013). *ISO/IEC 27001 - Information security management.* Obtenido de http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

ISO27000.es. (s.f.). *Consejos de implantación y métricas de ISO/IEC 27001 y 27002. 2007.* Obtenido de ISO27000.es: http://www.iso27000.es/download/ISO_27000_implementation_guidance_v1_Spanish.pdf

Jaramillo, O. (2008). *Estudio de los procesos de seguridad de la información.* Obtenido de http://repositorio.utp.edu.co/dspace/bitstream/11059/2370/1/0058S572.pdf

La auditoría interna como una herramienta para establecer controles internos eficientes en las pequeñas y medianas empresas ferreteras de la Ciudad de San Miguel, disponible en internet en: http://168.243.33.153/infolib/tesis/50107386.pdf

UNAD. (s.f.). *Riesgos y control informático.* Obtenido de http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_1_conceptos_de_vulnerabilidad_riesgo_y_amenaza.html

4.Contenido

INTRODUCCIÓN

Aún hoy día ya conocidos los riesgos de seguridad en las tecnologías de la información y comunicaciones (TICs), se encuentran empresas y organizaciones en las que se hace indispensable evaluar y establecer un sistema de gestión en seguridad de la información para preservar la disponibilidad, integridad y confidencialidad, de sus activos informáticos. Este proyecto de diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001:2013 y siguiendo la metodología MAGERIT para la empresa USOMET Ltda. en la ciudad de Ibagué para determinar cómo este resultado incrementa la seguridad para todos sus activos.

OBJETIVO GENERAL

Facilitar la administración de la seguridad informática y de la información mediante el diseño de un manual de políticas y procedimiento que apoyen el SGSI basado en la norma ISO/IEC 27001:2013 aumentando la competitividad de la empresa USOMET LTDA.

OBJETIVOS ESPECÍFICOS

Diagnosticar las condiciones actuales de la empresa USOMET Ltda., en lo relacionado en materia de información y seguridad informática, identificando sus activos informáticos,

mediante instrumentos de recolección de información.
Caracterizar los procesos y procedimientos de manejo de información en USOMET con el fin de evaluar e identificar las vulnerabilidades, amenazas y riesgos, relacionados con los activos informáticos.
Definir mecanismos de gestión de seguridad informático basados en la norma ISO/IEC 27001:2013 que faciliten la solución de problemas mediante la aplicación de políticas y procedimientos.
Diseñar el manual de políticas y procedimientos para el sistema de gestión de seguridad de la información.

ACTIVOS DE INFORMACIÓN

Se realizó el levantamiento de inventario referente a los activos que conforman el sistema de información de la empresa.

MEDIDAS DE SEGURIDAD

En labor conjunta con el personal de la empresa se estableció que medidas de seguridad aplican actualmente en referencia a los activos de información.

ANÁLISIS DE VULNERABILIDADES

Siguiendo la metodología MAGERIT se realizó la valoración de vulnerabilidades a las que están expuestos los activos inventariados.

GESTIÓN DEL RIESGO

Con el apoyo de la metodología MAGERIT y las normas ISO/IEC 27001:2013 y 27002, se estableció la valoración de amenazas, riesgo, impacto, objetivos de control y controles que consecuentemente con las valoraciones realizadas han de servir para incrementar el nivel de seguridad de los activos en la empresa.

POLÍTICAS DE SEGURIDAD

Realizado el análisis del panorama de riesgos, se procedió al diseño de la política de seguridad para que sea aprobada, socializada, puesta en práctica y actualizada periódicamente en la empresa.

5.Metodología

TIPO DE INVESTIGACIÓN

El paradigma de investigación es de tipo cuantitativo, ya que supone la medición de vulnerabilidades, amenazas y riesgos de seguridad de acuerdo a escalas de medición que indicados en la metodología MAGERIT para el análisis de riesgos.

Este tipo de investigación es descriptiva porque describe los procesos, servicios, activos

informáticos, las vulnerabilidades, amenazas y riesgos existentes en USOMET.

LÍNEA DE INVESTIGACIÓN

Se aplica la línea de investigación: gestión de sistemas que hace referencia a la indagación en sus dinamismos por medio de la evolución de las tecnologías de la información.

Para el logro de los objetivos propuestos se desarrollarán las siguientes actividades conforme cada objetivo.

Objetivo 1: Diagnosticar y evaluar las condiciones actuales de la empresa USOMET Ltda., en lo relacionado en materia de información y seguridad informática, identificando sus activos informáticos, mediante instrumentos de recolección de información.

Actividades:
- Realizar visitas a la empresa para identificar los activos informáticos existentes, registrando cada uno en los formatos prediseñados.
- Solicitar información sobre los inventarios de los activos informáticos.
- Entrevistar a los responsables del área informática para determinar los activos informáticos que soportan el sistema de información.

Objetivo 2: Caracterizar los procesos y procedimientos de manejo de información en USOMET con el fin de evaluar e identificar las vulnerabilidades, amenazas y riesgos, relacionados con los activos informáticos.

Actividades:
- Solicitar información sobre los funcionarios y procesos que cada uno realiza sobre los activos informáticos.
- Acompañar en su labor a los funcionarios que realizan actividades que involucran los activos informáticos.
- Registrar los hallazgos de vulnerabilidades, amenazas y riesgos, sobre su forma de uso en instrumentos de medición previamente diseñados.

Objetivo 3: Definir mecanismos de gestión de seguridad informático basados en la norma ISO/IEC 27001:2013 que faciliten la solución de problemas mediante la aplicación de políticas y procedimientos.

Actividades:
- Definir políticas de seguridad de la información para el manejo de los activos de la empresa.
- Establecer procedimientos de manejo apropiado para los diferentes tipos de activos identificados.
- Validar con la gerencia de USOMET las políticas y procedimientos generados.

Objetivo 4: Diseñar el manual de políticas y procedimientos para el sistema de gestión de seguridad de la información.

Actividades:
- Indicar controles a aplicar conforme el estudio realizado.
- Elaborar la política de seguridad.

6.Conclusiones

Las principales conclusiones obtenidas en esta investigación son:

• A la pregunta planteada en este proyecto se responde categóricamente que, con la elevación de nivel en sus medidas de seguridad para el sistema de información se incrementa el respaldo en el manejo de la información y por ende la competitividad de la empresa.

• Se observa alta disposición del personal de la empresa a conocer las valoraciones de seguridad obtenidas y poner en práctica la política de seguridad y los controles sugeridos.

• La gerencia de la empresa, reconoce la importancia de la valoración de los activos de información y ha brindado todo su respaldo en el desarrollo de este proyecto.

• La gerencia está comprometida con el logro de la concientización y capacitación periódica de todo el personal vinculado para mantener vigentes las medidas de seguridad.

• La gerencia de la empresa se reserva el derecho a establecer los procedimientos adecuados para cada control señalado, determinando si se realizará mediante dispositivos electrónicos de detección biométrica o asignando personal de seguridad o como corresponda siendo consecuente con el tamaño de la empresa y la disponibilidad de recursos económicos y de personal.

• La empresa considera cumplido el objetivo de este proyecto que eleva el nivel de seguridad del sistema de información y se compromete a aplicar las recomendaciones y mantener actualizada toda la documentación a fin de realizar la adopción y aplicación de las medidas de seguridad necesarias para asegurar sus activos.

Elaborado por:	HENAO, Jaime
Revisado por:	GONZÁLEZ, Salomón